

CyberCAN Washington:

A Regional Assessment of
Nonprofit Cybersecurity and
Strategic Recommendations
for Washington State



Shannon Pierson
Sarah Powazek
Nicholas Perematko

April 2026



Table of Contents

Executive Summary	4
CyberCAN Washington: Bridging the Gap Between Government and Nonprofits	6
Methodology	9
Findings	11
1. Quantifying the Impact of Cyberattacks	14
2. Understanding Nonprofit Cyber Hygiene	17
3. An Investment Gap for Nonprofits	22
4. The Digital Isolation of Nonprofits	27
Recommendations	32
Conclusion and Future Research	37
Acknowledgments	38



Executive Summary

The fact that nonprofits struggle with cybersecurity is widely acknowledged but poorly studied. The Center for Long-Term Cybersecurity's (CLTC) CyberCAN Washington project seeks to fill this gap by providing rigorous survey and interview data on the challenges nonprofits on the ground face regarding cybersecurity staffing, budgets, data protection, incident response, and other key indicators of cyber defense. In partnership with Washington Technology Solutions (WaTech), Washington State's premier agency providing enterprise information technology (IT) service, support, strategy, and security for Washington State public agencies and municipalities, CLTC adapted our 2023 survey with the City and County of San Francisco into a statewide nonprofit cybersecurity study for Washington.

also interviewed nonprofits and local government leaders so they could interpret the data in the context of subject matter experts' lived experiences. Survey respondents were primarily smaller nonprofit organizations, with over half employing fewer than 20 full-time employees and nearly a third employing fewer than five full-time employees.

These findings informed our recommendations for capable actors like Washington State, WaTech, and large cities and counties to play a greater role in nonprofit cybersecurity. CLTC recommends the following to improve nonprofit cybersecurity in Washington:

1. **Nonprofits should reduce the amount of sensitive data they collect.**
2. **City and county governments should play a coordinating role in connecting local nonprofits to cybersecurity resources that align with their budgets and needs.**
3. **The State of Washington should establish a short-term working group on nonprofit cybersecurity to define and operationalize local government coordination.**
4. **The State of Washington should include nonprofits in the full scope of support provided by centralized resources, such as the Washington Volunteer Cybersecurity Incident Response Team (CIRT).**
5. **The State of Washington and well-resourced city and county governments should offer shared cybersecurity tools and services to nonprofits.**
6. **The State of Washington should invest in expanding and strengthening supportive programs tailored to the cybersecurity needs of nonprofits.**

These recommendations were developed by CLTC alone based on our analysis of the survey and nonprofit interviews.

It is clear that without intervention, Washington nonprofits delivering social services will continue to face existential cybersecurity threats from which they may not recover. We urge the State of Washington and leading governments in Seattle, Redmond, Bellevue, Tacoma, and many other cities and counties to bring nonprofits under the umbrella of public entities receiving digital protections and cybersecurity support.

Four Main Findings

Through rigorous analysis, we uncovered four main findings for Washington-based nonprofits:

Finding #1:

Nonprofits frequently experience cyber-attacks that disrupt operations, cause financial losses, and expose sensitive data.

Finding #2:

Nonprofits carry significant cyber risk because they collect sensitive information and have limited adoption of essential cybersecurity controls.

Finding #3:

Nonprofits do not have the capacity to invest in cybersecurity due to insurmountable staffing and budget constraints—trends very likely to continue.

Finding #4:

Nonprofits struggle to prioritize cybersecurity until an incident occurs and lack the knowledge to make necessary improvements in the aftermath.

In total, CLTC surveyed 100 nonprofits with a robust methodology informed by Indiana's local government cybersecurity assessment program, CyberTrack. Researchers



CyberCAN Washington: Bridging the Gap Between Government and Nonprofits



How nonprofits boost city, county, and state resident services

Nonprofits serve as a critical extension of the public service delivery apparatus. States, counties, cities, and towns rely on nonprofits to deliver essential human services—such as homeless support, food access, and youth programs—that governments may not be best-positioned to provide directly. Nonprofits’ subject matter expertise, community trust, and local knowledge enable governments to reach and assist vulnerable populations. They can also provide these services at a fraction of what they would cost if state or local governments operated such programs themselves.

As a result, state and local governments regularly fund and contract with nonprofits as an extension of their public service delivery system, and these funds constitute a large portion of nonprofits’ funding.

Because nonprofits play such an integral role in delivering public services, local governments have a vested interest in the resilience and security of their nonprofit partners. City and county governments invest a great deal of time, training, and effort in nonprofit relationships to get them set up to deliver public services. Local governments cannot afford to lose these providers to devastating cyber incidents.

This report set out to help state and local governments better understand the current cybersecurity posture of nonprofits and identify where public and private sector support can most effectively intervene to strengthen nonprofit cyber resilience.

The need for high-fidelity nonprofit cybersecurity studies

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 among the most common targets of cyberattacks and among the least prepared to defend against them.¹ The Cybersecurity and Infrastructure Security Agency (CISA), the US’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.”²

Nonprofit cyberattacks hurt residents:

Cyberattacks on nonprofits cause immediate and serious damage. In 2020, a hunger relief organization in Philadelphia lost nearly \$1 million due to a cyberattack—funding that was intended to go toward building a new community kitchen facility.³ In 2022, cyber criminals stole records of more than 5000,000 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.⁴



1 Microsoft Security, *Microsoft Digital Defense Report 2021* (Microsoft, 2021).

2 U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA), *Mitigating Cyber Threats with Limited Resources: Guidance for Civil Society* (DHS, 2024).

3 Pat Ralph, “Philabundance Falls Victim to Cyberattack, Loses Almost \$1 Million,” *PhillyVoice*, 1 December 2020.

4 “Sophisticated Cyber Attack Targets Red Cross Red Crescent Data on 500,000 People,” International Committee of the Red Cross, 19 January 2022.

While nonprofit cybersecurity is a critical issue and a frequent topic of conversation in cybersecurity circles, there is a distinct lack of data available to quantify and describe the cybersecurity challenges nonprofits face. Existing studies largely focus on sentiment analysis, evaluating nonprofits' satisfaction, optimism, budget, and trust in technology through qualitative surveys and interviews.⁵ While such reports can provide helpful context, qualitative information about sentiment alone is not adequate 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 U.S. and Europe, focusing on factors such as their use of cybersecurity awareness training and the presence of security-related policies and procedures.⁶ Few studies, however, have focused on a regional set of nonprofits, attempting to understand their unique obstacles and relationships with their local government.

CyberCAN: Combining research and community building

CLTC's Cybersecurity for Communities and Nonprofits (CyberCAN) research initiative is designed to use research to bridge the gap between local government agencies and the nonprofits that serve their residents.⁷ The initiative helps deepen local governments' understanding of nonprofit cybersecurity challenges and identify opportunities to improve nonprofits' cyber defenses.

The first survey was launched in March 2024 through a partnership between CLTC and the City and County of San Francisco's Department of Technology and Office of Digital Equity. This partnership sought to explore how best to extend city and county information technology (IT) and cybersecurity resources to support struggling local nonprofits.

The team conducted a first-of-its-kind study of 68 San Francisco-based nonprofits to gather data on their cybersecurity needs, support preferences, available resources, and adoption rates of cybersecurity controls.

“Scammers are getting more and more sophisticated. We're doing our best, but it might be only a matter of time until something happens.”

Washington nonprofit providing support and funding to socially impactful startups



CLTC processed this data and released a report in November 2024 with key findings and actionable, tailored recommendations for how the city could better support local nonprofits in strengthening their cybersecurity defenses.⁸ The initiative culminated in a report launch event, where city staff engaged with the findings and began discussing ways to implement the proposed solutions.⁹

Since publishing this inaugural study, the CLTC team has refined its methodology and introduced an implementation component to directly connect state and local government and nonprofits with cybersecurity partners that can provide pro bono resources and hands-on support.

CLTC has recently broadened the scope of this research to the state level by partnering with the State of Washington's central IT and cybersecurity agency, Washington Technology Solutions (WaTech), to conduct a regional study of nonprofits located throughout the state. This study involved multiple components, including a survey designed to gather data on their cybersecurity challenges and interviews to better understand their experiences with cyberattacks. We used the data generated by the survey to identify ways in which state and local governments can extend their IT and cybersecurity resources to better support nonprofits, as well as to inform the State of Washington's broader cybersecurity policy and long-term cybersecurity strategy toward public interest organizations.

5 Salesforce, *Global Nonprofit Trends Report*, 5th ed. (Salesforce, 2022).

6 Robert Hulshof-Schmidt, *State of Nonprofit Cybersecurity* (NTEN, 2018); Alexandru Lazar, “Cyber-Poor, Target-Rich: The Crucial Role of Cybersecurity in Nonprofit Organizations,” Cyber Peace Institute, 25 March 2024; Christoffer Lindström, “Cybersecurity Experiences and Practices in Charities: A Qualitative and Quantitative Survey of Swedish Charities,” DiVA, 2022.

7 *CyberCAN: Cybersecurity for Cities and Nonprofits*, CLTC, UC Berkeley.

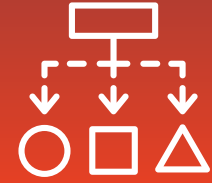
8 Sarah Powazek and Shannon Pierson, *CyberCAN: Cybersecurity for Cities and Nonprofits Strategic Recommendations for the City and County of San Francisco to Improve Nonprofit Cybersecurity* (CLTC, 2024).

9 “*CLTC and the City and County of San Francisco Launch CyberCAN*,” CLTC, December 2024.

The CyberCAN initiative is not just a survey; it is a model for engaging directly with nonprofits and local government leaders as integral stakeholders and laying the groundwork for long-term and sustainable cybersecurity communication between these communities. 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 state and local government decision-makers and nonprofit beneficiaries will be a replicable model for future collaborations between state and local government, nonprofits, and academic institutions.



Methodology



CLTC researchers designed and conducted a mixed methods study—involving both surveys and interviews—to collect quantitative and qualitative data on nonprofits’ current cybersecurity resourcing and preparedness, challenges, and most needed resources. These data were analyzed to derive descriptive findings, which informed policy recommendations for state and local governments.

Survey Scoping and Design

CLTC researchers built the Washington survey using an instrument originally developed during the first iteration of this study in 2024. To further refine our methodology, CLTC drew on the methodology developed by Indiana University’s Center for Applied Cybersecurity Research (IU CACR) and Purdue University’s cyberTAP for CyberTrack, Indiana’s Local Government Cybersecurity Assessment Program.¹⁰ The CyberTrack methodology involves assessment of an evidence-based prioritized subset of two cybersecurity frameworks, proven to be the most effective controls at preventing or limiting the impact of cyberattacks:

- (1) the Trusted CI Framework and
- (2) Center for Internet Security (CIS) Critical Security Controls Implementation Group 1 (IG1), Version 8.1.

From these controls, CLTC researchers selected those determined to be most relevant and achievable for nonprofits. This selection was informed by our prior research into the distinctive cybersecurity needs and challenges nonprofits faced and was kept narrow to ensure concise and accessible survey results for nonprofits.

Survey Overview

The survey is divided into four sections:

- (1) Demographics,
- (2) Cybersecurity Program Maturity,
- (3) Cyber Hygiene Practices, and
- (4) Desired Support.

Section 1 collected information to paint a picture of nonprofits included in the sample. Questions focused on basic characteristics of each organization, such as geographic location, primary mission, the types of services provided, and communities served.

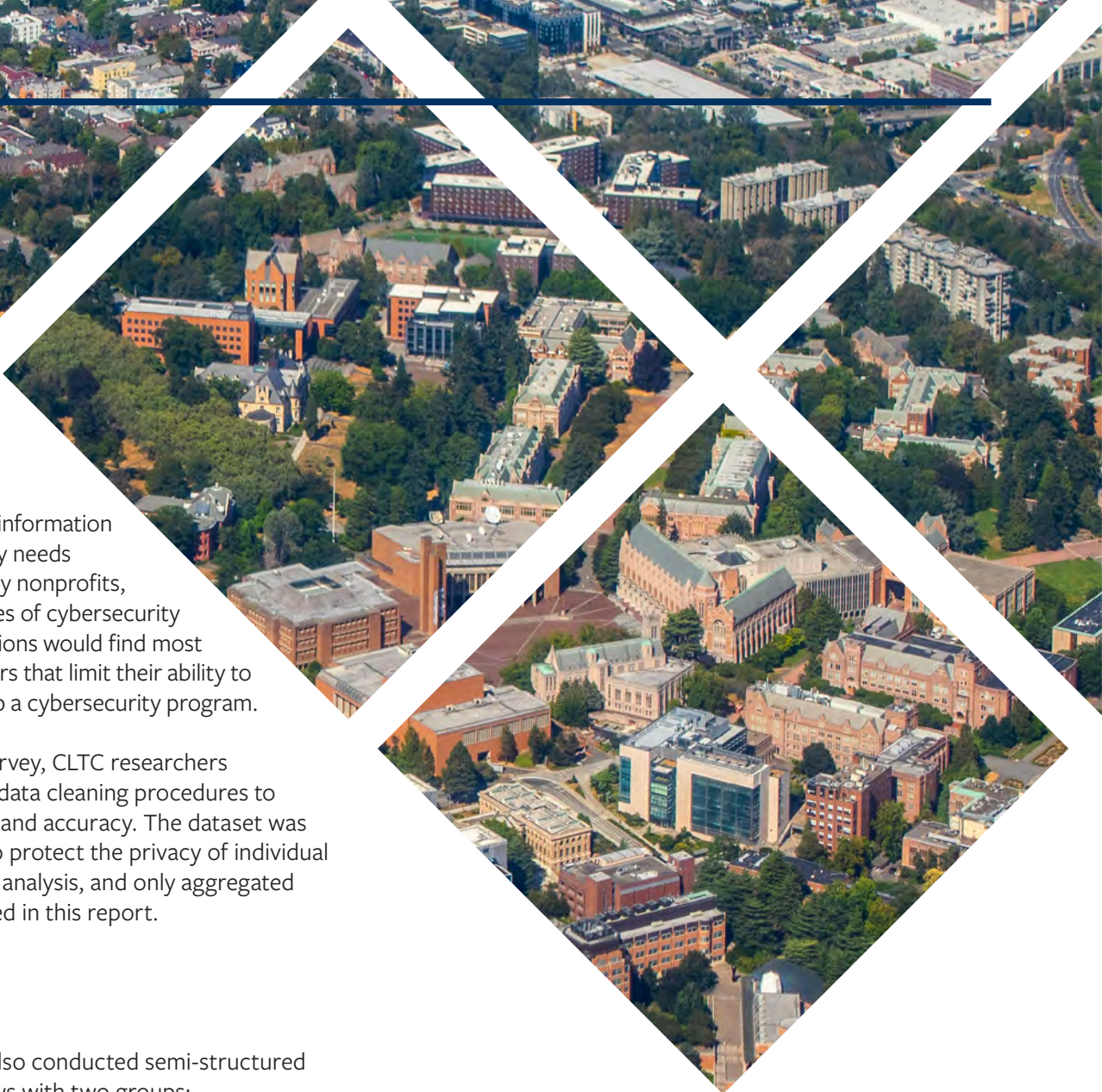
Section 2 gathered information on the current status and capacity of nonprofits’ cybersecurity programs. Questions addressed key components of cybersecurity resourcing and governance, including budget, personnel, and leadership.

Section 3 measured nonprofits’ implementation of several essential, high-impact cybersecurity controls and captured details of their experiences with cyber incidents and preparedness for incident response. Questions examined data collection and retention practices, deployment of multi-factor authentication (MFA), and account privileges. These measures were derived from the nonprofit-relevant subset of CIS Controls identified in IU CACR’s “Transformative Twelve,”¹¹ including Safeguards 3.4: Enforce Data Retention; 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts; 6.3: Require MFA for Externally-Exposed Applications; 6.5: Require MFA for Administrative Access; and 11.4: Establish and Maintain an Isolated Instance of Recovery Data.¹² The section also asked about cyberattacks experienced, their impacts, and whether organizations had incident response plans or cyber insurance in place for recovery.

¹⁰ [IU CACR, cyberTAP, Purdue University, Indiana Cybertrack Program](#)

¹¹ [“Applying a Practical, Evidence-Based Approach to Cybersecurity Controls,” IU CACR.](#)

¹² [CIS Critical Security Controls.](#)



Section 4 collected information on the cybersecurity needs and barriers faced by nonprofits, focusing on the types of cybersecurity resources organizations would find most useful and the factors that limit their ability to prioritize building up a cybersecurity program.

After closing the survey, CLTC researchers conducted routine data cleaning procedures to ensure data quality and accuracy. The dataset was then anonymized to protect the privacy of individual participants before analysis, and only aggregated results are presented in this report.

Interviews

CLTC researchers also conducted semi-structured qualitative interviews with two groups:

- (1) nonprofits that experienced cyber incidents and
- (2) city and county personnel working in IT and human services.

We interviewed three nonprofits that had experienced major cyber incidents to generate insights into their impacts on nonprofit organizations. Interviews explored how incidents were discovered and handled; timelines for response and recovery; and short- and long-term impacts on operations, finances, data security, and relationships with donors and beneficiaries. Interviews also collected information on resulting changes to cybersecurity practices.

In addition, we interviewed eight city and county personnel to examine the role of local government in supporting nonprofit cybersecurity. Participants included five IT departments and three human services departments from four Washington counties and two

cities. Interviews examined the extent to which these departments:

- (1) interact with nonprofits,
- (2) are aware of and respond to nonprofit cybersecurity risks,
- (3) see a role for local and state government in addressing these risks, and
- (4) identify resources that could help address the challenge.

These interviews provided insight into both the technical and the operational relationships between local government and nonprofits and helped to inform our policy recommendations.



Findings

Summary Statistics: Which Types of Nonprofits Were Surveyed?

CLTC researchers surveyed 100 nonprofits across Washington State. Responses came from geographically and demographically diverse regions, including high-density urban counties such as King County and less populated rural counties like San Juan and Clallam.

In total, nonprofits from 21 of Washington’s 39 counties (54%) were represented. The largest share of responses came from (1) King County, (2) Clark County, and (3) Snohomish County, which was expected given they are among the most populous counties in the state.

93% of surveyed nonprofits serve primarily within Washington State, reaching approximately **1.9 million** people with their services.

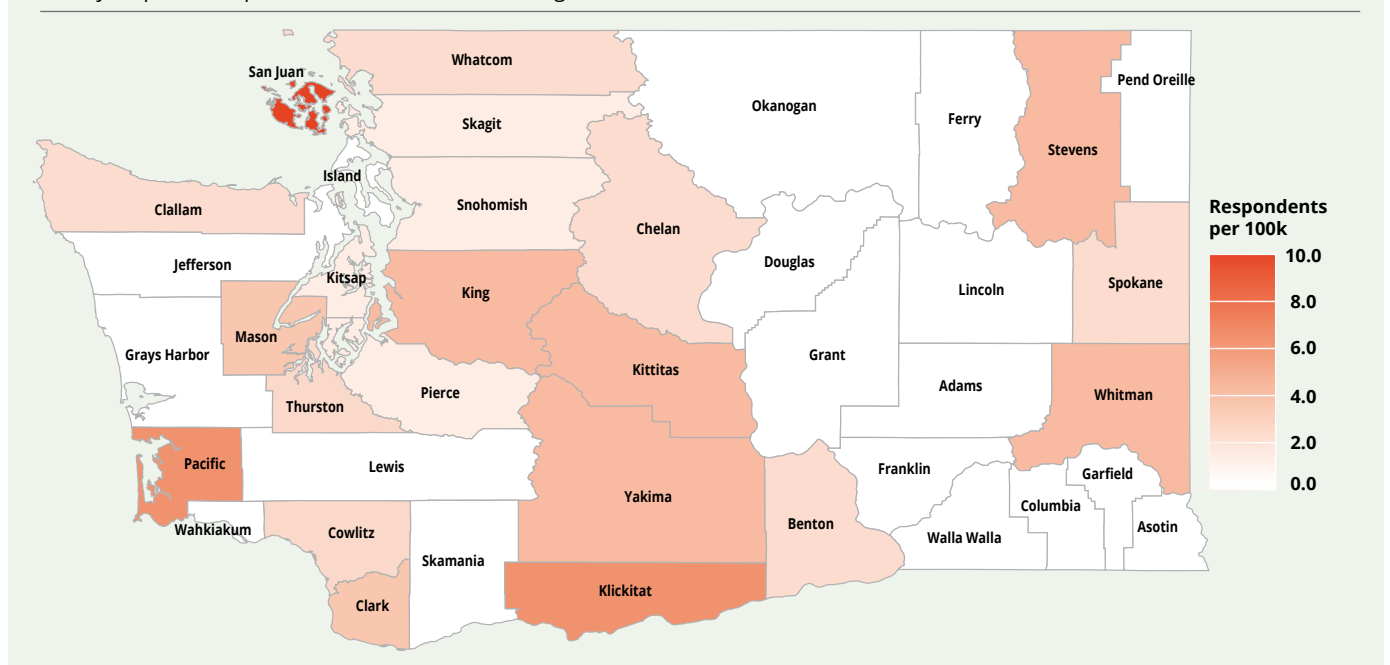
Top counties represented in the survey:

- (1) King County
- (2) Clark County
- (3) Snohomish County

61% of surveyed nonprofits employ fewer than **20 full-time staff**.

Figure 1: Nonprofit Survey Representation by County (Per Capita)

Survey respondents per 100,000 residents—Washington State



The sample primarily consists of smaller nonprofit organizations, with over half (61%) employing fewer than 20 full-time staff and nearly a third (31.3%) employing fewer than five full-time staff. Medium (14%), large (16%), and very large organizations (8%) make up the remainder of the respondent pool. Respondents manage

sizable annual operating budgets: the average budget (excluding values about the 95th percentile to reduce skew from a small number of high-budget outliers) is \$3.66 million, but 33% of organizations report budgets under \$1 million in 2025.

Figure 2: Size Distribution of Nonprofits, By Number of Full-Time Staff

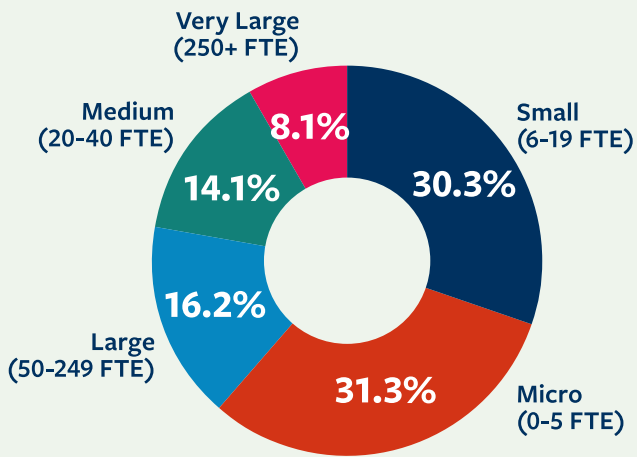
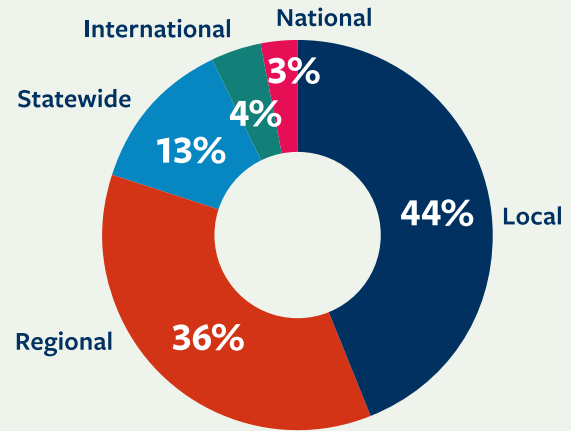


Figure 3: Primary Geographic Service Area of Nonprofits¹³



Top Services Delivered

1 Youth Development

2 Family Support Services

3 Food Access

4 Community Improvement & Development

5 (Tied) Workforce Development & Employment Services AND Housing & Homelessness Services

These nonprofits serve almost entirely within Washington State (93%) and operate at a highly local level—either within a single city or county (44%) or regionally across multiple cities or counties (36%).

This population of nonprofits is heavily engaged in delivering direct services to individuals and communities (66%), meaning they provide immediate, frontline assistance to people in need. Respondents reported delivering a variety of essential services across Washington. The most common service area was Human Services (30%), followed by Education & Workforce Development (20%) and Civil Rights & Advocacy (15%), among others.

Within those service areas, 31 unique services were represented in total, ranging from small business support to substance abuse support to legal aid. The services nonprofits most frequently provided helped some of the most vulnerable members of these communities: children,

struggling families, the food insecure, the unemployed, and the housing insecure. Top services included (1) youth development (e.g., after-school and summer programs, mentoring, youth leadership initiatives), (2) family support (e.g., childcare, parenting classes, family counselling, baby supplies), and (3) food access (e.g., food pantries, free meal programs).

State and local governments regularly fund and contract with nonprofits as an extension of their public service delivery system, providing a substantial portion of nonprofits' funding. For the nonprofits surveyed, grants and contracts, mainly from local and state governments, account for a bulk of their total income. Among the nonprofits that receive grant funding (89%), 70% receive grants from local governments and 67% from state governments. Among the 56% of nonprofits that receive funding from contracts, 84% receive contract funds from local government agencies and 70% receive them from the state.

¹³ Note: "Local" refers to nonprofits serving individuals located within city or county limits. "Regional" refers to nonprofits serving individuals located in multiple cities or counties within a state or area.

Figure 4: Sources of Funding for Nonprofits

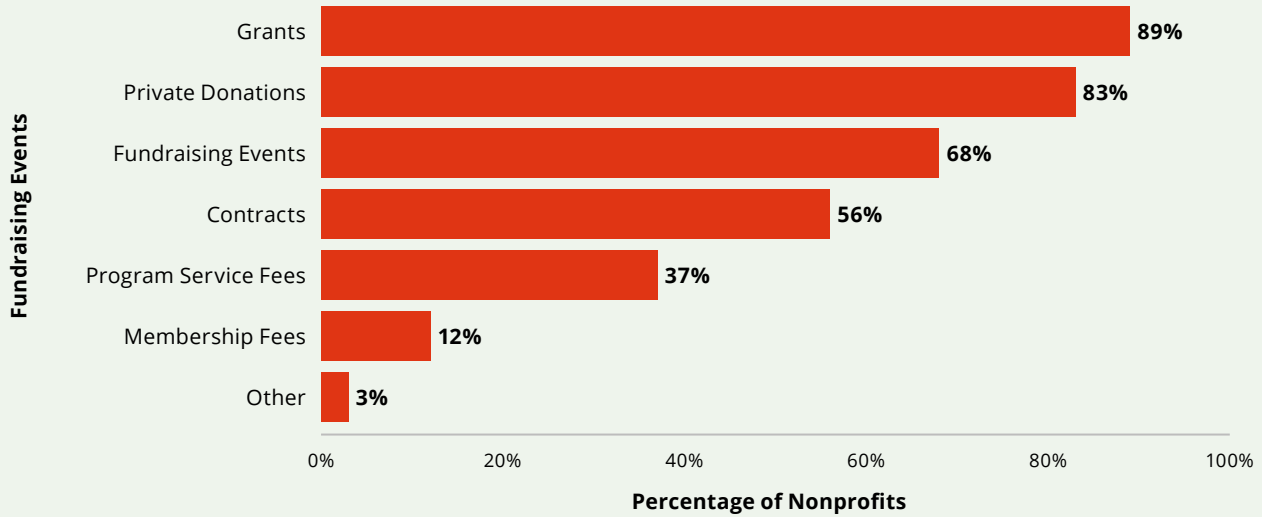
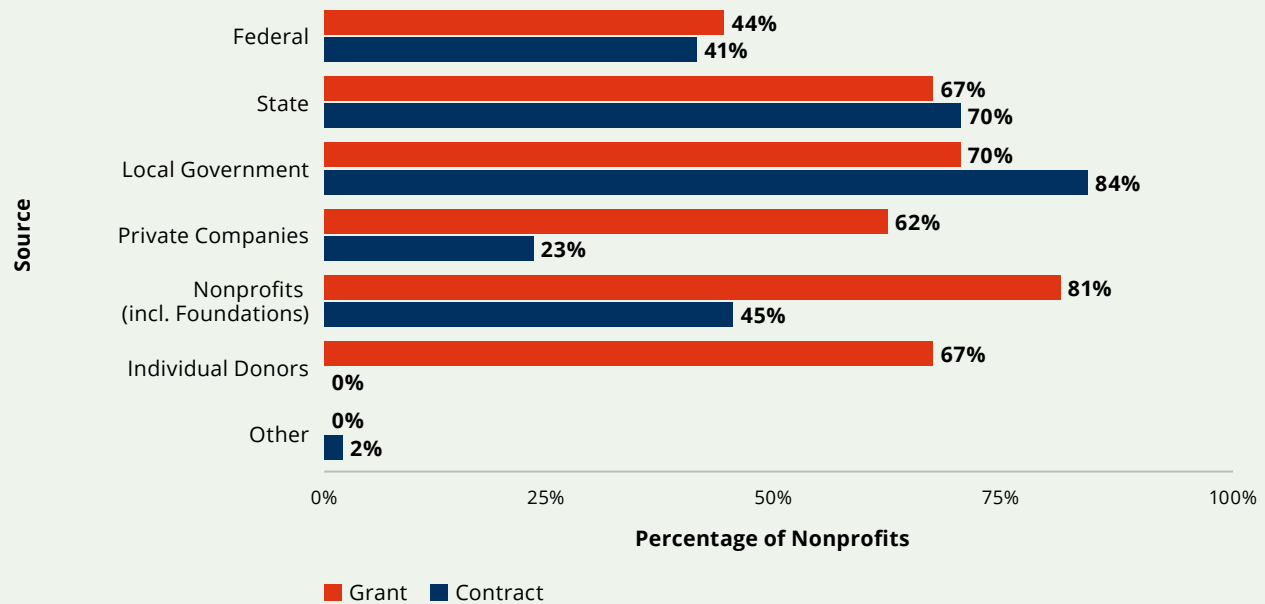


Figure 5: Sources of Grant and Contract Funding For Nonprofits¹⁴



The services of these nonprofits cumulatively reach approximately 1.9 million people in Washington State, the equivalent of roughly 23% of the state’s population.¹⁵ They require approximately 15,700 volunteers to execute on their missions of helping others.

¹⁴ Note: “Local” refers to nonprofits serving individuals located within city or county limits. “Regional” refers to nonprofits serving individuals located in multiple cities or counties within a state or area.

¹⁵ Note: This figure includes cumulative service reach reported by nonprofit organizations and may include individuals served by more than one nonprofit.

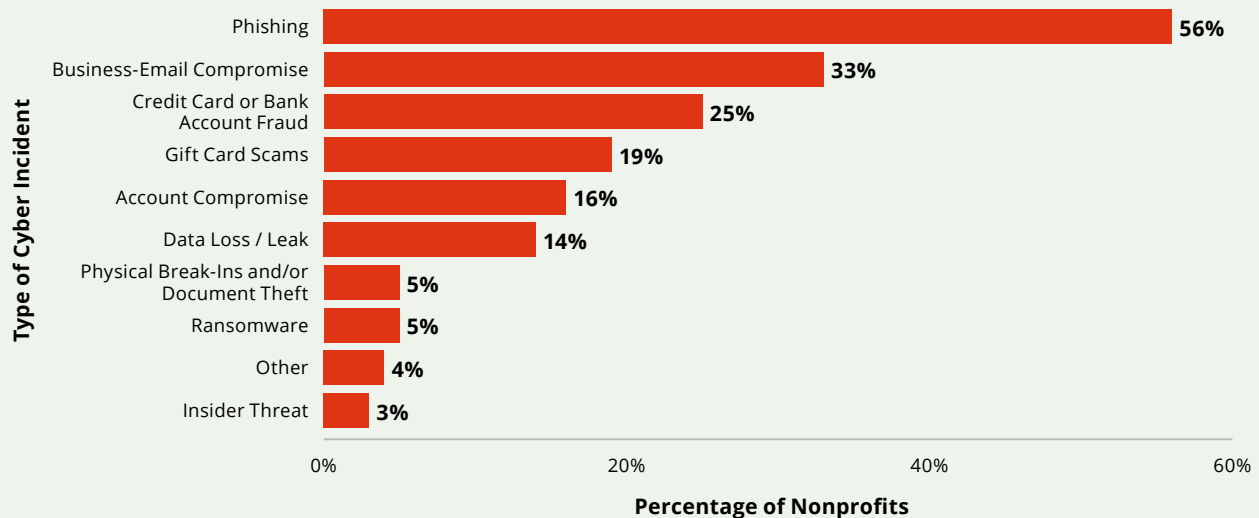
1. Quantifying the Impact of Cyberattacks

Finding #1:

Nonprofits frequently experience cyberattacks that disrupt operations, cause financial losses, and expose sensitive data.

Cybercrime targeting Washington nonprofits is widespread, with hackers most commonly gaining access through email-based attacks.

Figure 6: Types of Cyberattacks Experienced by Nonprofits Within the Last Three Years
[79 Responses in Total]



Survey results show a prevalence of cyberattacks targeting Washington nonprofits: 79% of nonprofits had experienced at least one attack in the previous three years. Email-based attacks were the primary

method used to gain access to a nonprofit’s digital assets, with phishing and business email compromise (BEC) emerging as the two most common onslaughts experienced.

79%

of nonprofits had experienced at least one attack in the previous three years.



The #1 attack method

against nonprofits were email-based attacks, including phishing and business email compromise (BEC).



Email-based attacks can be particularly damaging to nonprofits because staff often exchange sensitive information and conduct financial transactions through email. In interviews, Washington nonprofits reported transmitting purchase orders and invoices, bank routing and account details, and spreadsheets containing sensitive client and donor data—and in some cases organizational passwords—via email. Once attackers gain access to an email account, they can review past communications to identify financial processes and sensitive data for executing follow-on scams. For example, CLTC researchers interviewed two nonprofits whose business email accounts were compromised and used by cybercriminals to steal bank account passwords or impersonate trusted vendors to steal funds. Consistent with interview data indicating that financial crimes can follow a breach, survey data also showed that credit card and bank account fraud ranked third among the most common cyber incidents reported by Washington nonprofits.

“When we inspected the email further, we saw that the email address was changed by one character. That’s all it took.”

Washington nonprofit providing housing, family, and employment support services

What Happened:

Attackers gained access to staff email accounts and reviewed prior correspondence related to vendor payments. They then impersonated a trusted vendor by spoofing its email address through typosquatting and asked to update their banking information for service payments. Believing the request was legitimate, the nonprofit transferred a **\$300,000** payment to the fraudulent account. The fraud was discovered when the legitimate vendor reported the payment had not been received, prompting the nonprofit to contact its cybersecurity insurance provider, who reimbursed \$200,000 of the loss.

Cyberattacks caused operational disruptions, lost funds, and data breaches for Washington nonprofits.

For nonprofits and their beneficiaries, the material impact of an incident can be especially severe. Most nonprofits operate on lean budgets, with little capacity to absorb financial losses, cover recovery costs, or withstand reputational damage that could jeopardize relationships with funders. Nonprofits also have low tolerance for service disruption; they provide essential community services like food aid, legal and housing assistance, and outreach that must operate continuously. When a nonprofit’s internal systems are compromised, service delivery can be halted, hurting vulnerable communities that depend on nonprofits for support.

Of nonprofits who experienced a cyber attack,

17%

lost funds with losses ranging from

\$200 to \$300,000



CLTC found that cyberattacks primarily caused operational disruptions, lost funds, and data breaches for Washington nonprofits. Among the nonprofits attacked, 34% reported operational disruptions, 17% experienced a loss of funds, and 12% suffered subsequent data breaches. Other impacts included breach of sensitive data, unauthorized access to sensitive accounts, and reputational damage.

Cyberattacks caused various types of operational disruptions for nonprofits. Most commonly, nonprofits reported that the greatest operational disruption resulted from the diversion of staff resources away from regular operations. According to our interviews, staff had to put their regular work activities on hold to handle remediation and response tasks, such as investigating the breach, coordinating with banks and legal counsel, and reporting the crime to law enforcement.

Some nonprofits had to navigate the cyber incident recovery process without the assistance of IT professionals or cybersecurity insurance. In some cases, this burden fell entirely on non-technical administrative staff, whose roles are unrelated to cybersecurity. One nonprofit interviewed by CLTC researchers described how their program director personally led an investigation and response effort into a major cyber incident because the organization had no IT or cybersecurity staff and no process in place for contacting a cybersecurity consultant for assistance. Circumstances like these stretch a nonprofit's organizational capacity to its limit as leaders struggle to manage the attack and restore normal operations. Numerous Washington nonprofits also reported credit and debit card fraud, bank account fraud, and gift card scams, with losses ranging from \$200 to \$300,000. Cyber criminals used stolen bank information to make unauthorized withdrawals, diverted employee paychecks to alternate accounts, and impersonated vendors in order to redirect payments into fraudulent bank accounts. In some cases, organizations recovered stolen funds by contacting their banks. In other cases, losses could not be reversed, forcing nonprofits to absorb the costs.

This is an outcome not every nonprofit can withstand. For example, a small Washington nonprofit providing addiction and homelessness services suffered a BEC attack, which led to an attempted fraudulent bank transfer that would have resulted in the withdrawal of nearly all of its funds. The staff described how the event affected them: "If we had lost that money, I don't know if we would have been able to continue to exist."

"If we had lost that money, I don't know if we would have been able to continue to exist. We were a young organization. We had no [financial] reserves, and it was a substantial amount of money. We got very lucky."

Washington nonprofit providing addiction and homelessness services

What Happened:

Attackers acquired access to the executive director's email and found a spreadsheet containing all major organizational passwords, sent as an attachment. Using those credentials, they accessed the nonprofit's bank account and initiated a transfer of **nearly all of its funds**. To conceal their activity, hackers set email filters that auto sent all bank alerts to the trash. The nonprofit discovered the fraud in time, canceled the transfer, and worked with the bank to return the money.

2. Understanding Nonprofit Cyber Hygiene

Finding #2:

Nonprofits carry significant cyber risk because they collect sensitive information and have limited adoption of essential cybersecurity controls.

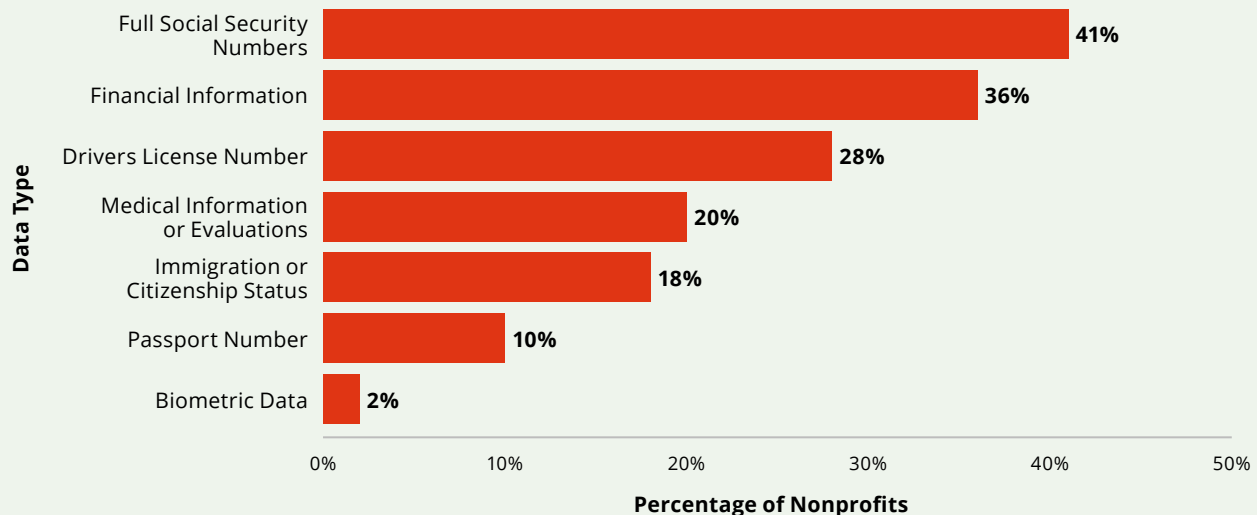
Washington’s nonprofits store highly sensitive data about clients and donors, making them attractive targets for cybercriminals and data breaches.

Nonprofits address basic critical needs like healthcare, housing, food access, childcare, and utility assistance for vulnerable populations. To deliver these services, they collect and store personally identifiable information (PII) about clients and donors. The National Institute of Standards and Technology (NIST) defines PII as “any information about an individual... that can be used to distinguish or trace an individual’s identity... and any other information that is linked or linkable to an individual.”¹⁶ Some examples of PII are name, social security number, date and

place of birth, biometric records, and other medical, educational, financial, and employment information.

CLTC found that Washington nonprofits handle a variety of PII, some of it highly sensitive. Most organizations reported collecting lower-risk data such as full names (91%), contact information (87%), addresses (81%), and birthdates (64%). More concerningly, over half of all nonprofits surveyed also stored “highly sensitive” identifiers (57%), such as social security numbers (41%), financial information (36%), and medical information or evaluations (20%). Several organizations even reported collecting immigration or citizenship status (18%) and passport numbers (10%)—information that could expose undocumented Americans to significant harm if compromised.¹⁷

Figure 7: Highly Sensitive Information Collected and Stored by Nonprofits



16 U.S. Department of Commerce, [Guide to Protecting the Confidentiality of Personally Identifiable Information \(PII\): Recommendations of the National Institute of Standards and Technology](#), by Erika McCallister et al., NIST Special Publication 800-122 (NIST, 2010).

17 Johana Bhuiyan, [“US Immigration Agency Explores Data Loophole to Obtain Information on Deportation Targets”](#) The Guardian, 20 April 2022.

Due in part to the sensitive data they hold, nonprofits are attractive targets for cybercrime.¹⁸ Consistent with this trend, CLTC researchers found that nonprofits that stored “highly sensitive” PII experienced a higher rate of cyber incidents (37%) compared to organizations that did not hold such information (27%). Data loss and leaks accounted for 8% of all cyberattacks experienced by nonprofits.

PII is valuable to commercial cyber criminals because they can profit off of it. There is a burgeoning underground market on the dark web built around stealing, trading, and monetizing PII by using it to commit financial fraud or extortion or by selling it to another bad actor.¹⁹ Stolen PII can be used for various types of identity fraud (e.g., opening accounts and applying for loans or credit cards under a false identity) or to make fraudulent purchases.²⁰ Even nonprofits with small budgets can contain financially valuable PII for cyber criminals.

Risky info:

Nonprofits that stored “highly sensitive” PII were more likely to experience a cyberattack than other nonprofits.



This issue has implications for state and local governments that fund or contract with nonprofits to deliver services. In interviews with state and local governments, respondents expressed concerns about the security and privacy of personal or residential data collected by the nonprofits. A cyber incident affecting a nonprofit may expose sensitive information about the very populations publicly funded services are intended to protect.

Washington’s nonprofits demonstrate moderate adoption of some of the most essential and effective cybersecurity controls.

More than half of Washington nonprofits report implementing two essential data protection practices:

- (1) periodically deleting sensitive data (55%) and
- (2) maintaining an isolated instance of recovery data (60%), also known as a secure data backup.

These controls help enable organizations to recover their organizational data and operations quickly after incidents such as ransomware, system failure, and accidental data loss.

However, nonprofits often do not institutionalize these practices. Fifty-five percent of nonprofits lack a formal retention policy. Without a policy establishing a process for deleting or archiving sensitive data with clear minimum and maximum retention timelines, these practices may be applied inconsistently. Holding onto sensitive information for longer than necessary increases these organizations’ risk of exposure if systems are compromised.

Backup gap:

Four in ten nonprofits do not have separate, secure backups of important data.



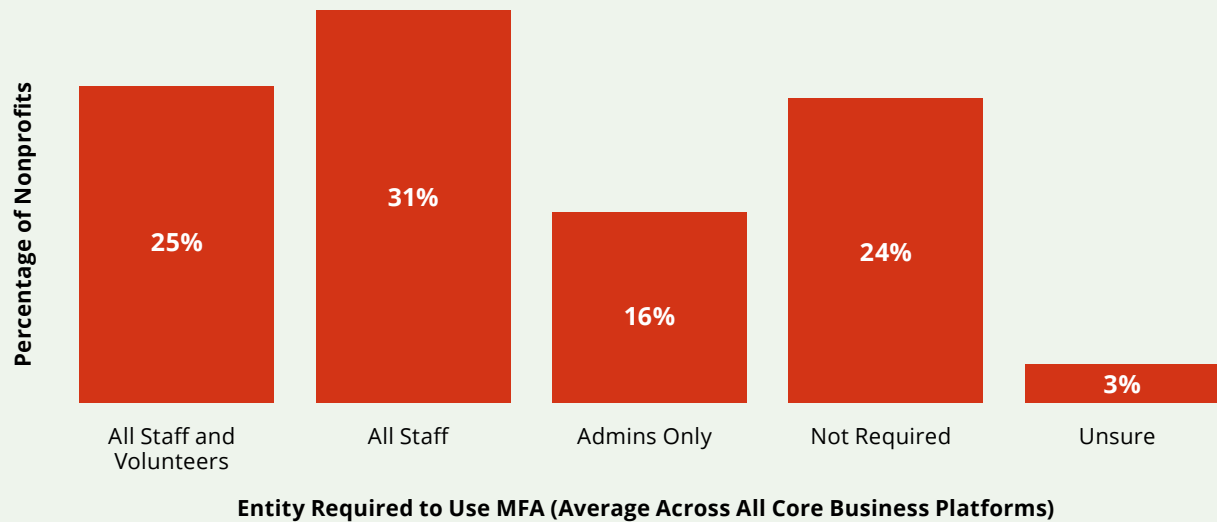
Notably, nonprofits have higher rates of adoption of secure backups than of sensitive data deletion. Sixty percent of nonprofits maintain a separate, secure backup of important data and update it frequently: 46% daily, 9% more than once per day, and 10% weekly. This suggests that many nonprofits recognize the importance of this practice. Still, with four in ten nonprofits lacking secure backups altogether, there remains a pronounced gap in basic cyber defenses for Washington nonprofits.

¹⁸ Microsoft Security, *Microsoft Digital Defense Report 2021*.

¹⁹ Ben Luthi, “*Here’s What Your Data Sells for on the Dark Web*,” Experian, 30 June 2025.

²⁰ “*Your Tax Forms Sell for \$20 on the Dark Web*,” Malwarebytes Labs, 19 March 2026.

Figure 8: Average MFA Requirements Across Nonprofits' Core Business Systems²¹



CLTC researchers found high levels of MFA usage across most software tools that nonprofits used. MFA is largely enabled by nonprofits on email (73%), collaboration tools (67%), customer relationship management platforms (74%), and cloud storage platforms (75%).²² Roughly a quarter of nonprofits reported making MFA mandatory for all employees and volunteers, a best practice for cybersecurity, while about 30% required it for staff only. Just 10% of Washington nonprofits reported not using MFA for any platform whatsoever. This finding suggests that Washington nonprofits have begun to adopt MFA as a basic security control.

These results were surprising given the relatively high rates of phishing and BEC reported elsewhere in the survey. MFA is widely recognized as one of the most effective defenses against account compromise, yet implementation is often challenging for smaller, resource-constrained nonprofits that lack IT staff.

CLTC researchers also found that MFA adoption produced different outcomes for Washington nonprofits. Based on our data, organizations that had implemented MFA experienced fewer phishing and

MFA works:

Nonprofits that had implemented MFA experienced fewer phishing and business email compromise attacks than nonprofits that had not.

business email compromise attacks. Although phishing and BEC incidents still occurred among organizations using MFA, the proportion of organizations experiencing incidents appears slightly lower among those with MFA compared to organizations without it. As a note, not all phishing attacks resulted in BEC incidents and not all BEC incidents stemmed from phishing attacks. MFA is a major preventative tool to combat BEC incidents and an effective safety measure against phishing attacks, but it should be understood that phishing attacks were reported in this study regardless of if they were ultimately successful in leading to further compromise.

²¹ Note: Nonprofits' core business systems include: email and productivity tools (e.g., Gmail, Microsoft 365); collaboration and communication tools (e.g., Slack, Teams); donor management or customer relationship management (CRM) platforms; cloud file storage platforms and document sharing (e.g., Google Drive, Dropbox).

²² Note: To produce these percentages on "Largely enabled," CLTC researchers combined adoption rates across three groups: (1) all staff and volunteers, (2) all staff, and (3) admins only.

Washington’s nonprofits are unprepared to respond to and recover from cyber incidents due to limited advanced planning and low adoption of cyber insurance.

Cybersecurity professionals and established frameworks consistently identify several core risk management practices that help organizations prepare for, respond to, and recover from cyber incidents. These include developing incident response plans, establishing business continuity plans, and obtaining cyber insurance.

When asked about these preparedness measures, most Washington nonprofits reported not having them in place. More than half (55%) had no incident response plan, nearly half (49%) lacked a business continuity plan, and 39% did not carry cyber insurance. There were also notable levels of uncertainty: 12% were unsure about the existence of an incident response plan and 12% about a business continuity plan, while 22% of nonprofits reported not knowing whether they had cyber insurance.

Figure 9: Incident Response Measures Definitions

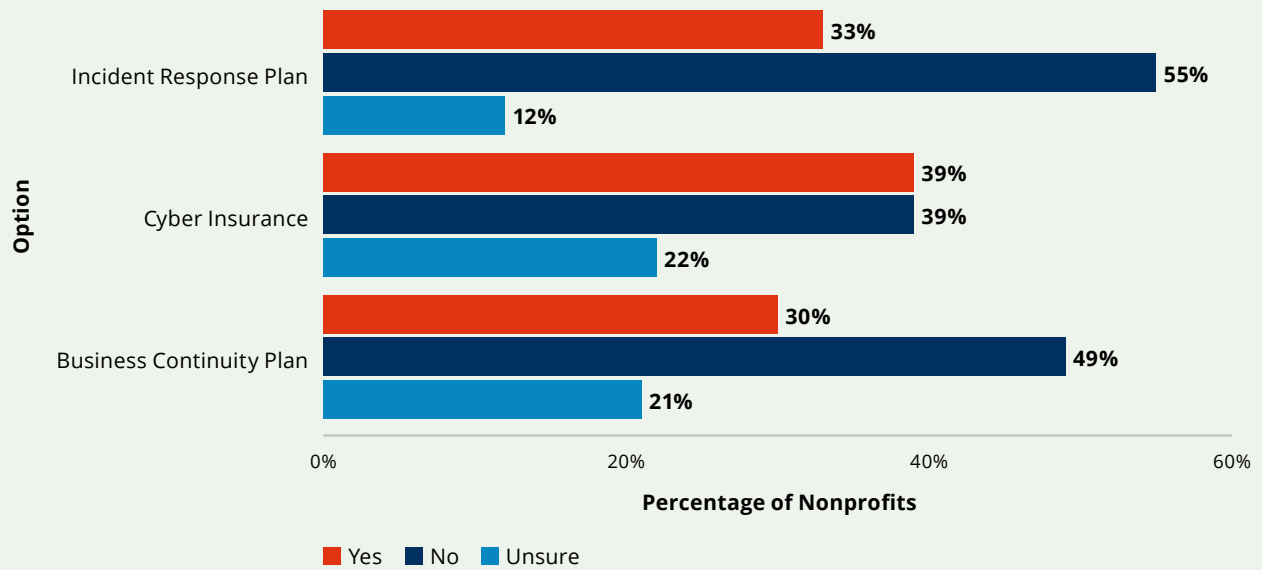
<p>Incident Response Plans</p>	<p>The documentation of a predetermined set of instructions or procedures for detecting, responding to, and minimizing consequences of a malicious cyberattack against an organization’s information systems(s).²³</p>
<p>Business Continuity Plans</p>	<p>The documentation of a predetermined set of instructions or procedures that describe how an organization’s mission/business processes will be sustained during and after a significant cyber disruption.²⁴</p>
<p>Cyber Insurance</p>	<p>A type of insurance that transfers a policyholder’s financial liability to cybersecurity and privacy events such as cyberattacks, data breaches, acts of cyberterrorism, and regulatory violations.²⁵</p>

23 U.S. Department of Commerce, *Contingency Planning Guide for Federal Information Systems*, by Marianne Swanson et al., NIST Special Publication 800-34 (NIST, 2010).

24 Swanson et al., *Contingency Planning Guide for Federal Information Systems*.

25 Narendran Vaideeswaran, “*Cybersecurity Explained*,” CrowdStrike, 21 February 2024.

Figure 10: Uptake of Incident Response Resources



These results suggest that many Washington nonprofits lack foundational materials needed to respond to and recover from cyber incidents, or to keep operations running during disruptions. This is especially concerning for nonprofits that are part of the emergency response apparatuses of states, counties, and cities. The cyber capacity constraints of nonprofits identified throughout this report, including limited cybersecurity expertise, staffing, and financial resources, likely contribute to underinvestment in planning and risk management.

The moderate levels of uncertainty also point to an organizational awareness gap. Even among organizations that have implemented incident response planning and resilience measures, staff appear moderately unfamiliar with them—indicating that the procedures may not be consistently communicated or operationalized by leadership.

3. An Investment Gap for Nonprofits

Finding #3:

Nonprofits do not have the capacity to invest in cybersecurity due to insurmountable staffing and budget constraints, trends very likely to continue.

Why IT staffing is critical to cybersecurity

Full-time IT headcount influences a nonprofit’s ability to understand and implement a cybersecurity program for the organization. Despite the cybersecurity field’s emphasis on purchasing technology to implement cybersecurity controls—the industry analysis site IT Harvest tracks over 10,000 cybersecurity products alone²⁶— people are integral to implementing a cybersecurity strategy within an organization. Full-time IT staff, sometimes with the additional support of managed services like IT and cybersecurity monitoring and detection, ensure that the nonprofit implements security controls, tailors and configures products to its organizational needs, and executes the day-to-day work of protecting user accounts from unauthorized access.

Nonprofits are at a critical inflection point for ensuring proper staffing organization-wide. A 2025 Urban Institute survey²⁷ found that 7% of nonprofits were planning to increase layoffs, more than double the number of nonprofits planning layoffs less than a year earlier. And, as shared in the summary statistics of this report, many nonprofits in Washington already have extremely small headcounts; over half of the nonprofits surveyed have fewer than 20 full-time staff members, and nearly a third (31.3%) have fewer than 5 full-time employees.

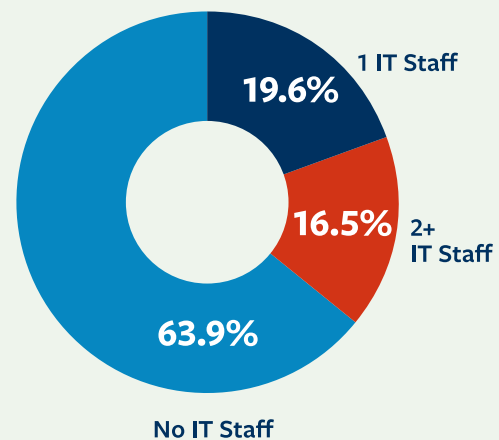
Results show nonprofits are severely lacking in full-time staff.

64%
of nonprofits have no full-time IT staff

1.57:
Average number of full-time IT or cybersecurity staff



Figure 11: Nonprofit Dedicated IT Staff



²⁶ IT Harvest.

²⁷ Laura Tomasko et al., How Government Funding Disruptions Affected Nonprofits in Early 2025: Nationally Representative Findings from the Nonprofit Trends and Impacts Study (Urban Institute, 2025).

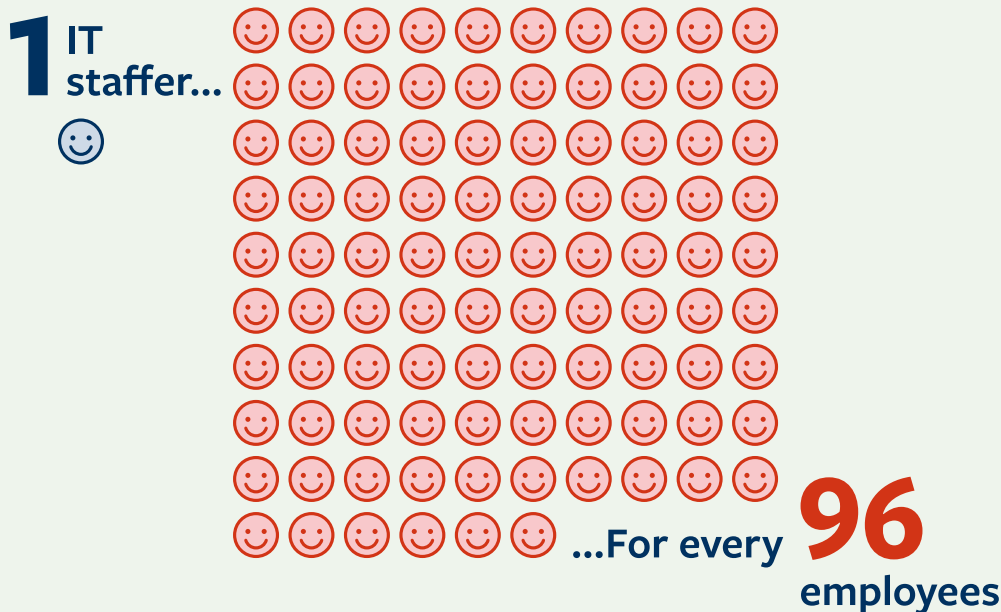
Survey results showed that nonprofits face severe staffing constraints. A majority of nonprofits (64%) do not employ any full-time IT staff. This does not mean that no one in the organization is handling cybersecurity responsibilities; nearly this same number (65%) shared that a staff member within their organization was taking on IT or cybersecurity duties even though it was not their primary job description. This finding is not surprising, as nonprofits have no real choice but to be online in order to provide services to the public, take in donations, and connect with their beneficiaries. The responsibilities for IT and cybersecurity must fall to someone within the organization, even if they are already shouldering another full-time role.

Nonprofits surveyed employed an average of 1.57 full-time IT staff total, a vanishingly small number even considering that many of the nonprofits are small to begin with. To add context, nonprofits have an average ratio of 1 full-time IT staff member to 96 full-time and part-time employees. This means that each full-time IT or cyber staffer—if there is one—is

responsible for securing the accounts and handling the incidents of an average of 96 other people within the organization, representing an enormous workload for a single or handful of IT experts.

To put this into perspective, a 2017 NTEN report on nonprofit IT staffing found that the average IT staffer supported 24 other employees, compared to 96 in our survey.²⁸ We found that Washington-based nonprofits are responsible for securing, on average, more than triple the number of employees the most comparable nationwide data available suggests. This is the exact same average we found in our previous 2024 CyberCAN San Francisco study: 1 IT staffer for every 96 employees at San Francisco-based nonprofits. This estimate likely understates the true burden, as it does not account for the addition of volunteers, whom many nonprofits rely on to carry out their services, increasing the number of employees for IT staff to manage by an average of 162. Despite this strain, this trend of severe understaffing in IT and cybersecurity is likely to continue, as nearly all surveyed nonprofits (91%) do not have any plans to hire additional IT personnel.

Figure 12: Nonprofits had an average of 1 IT staffer for every 96 full and part-time employees



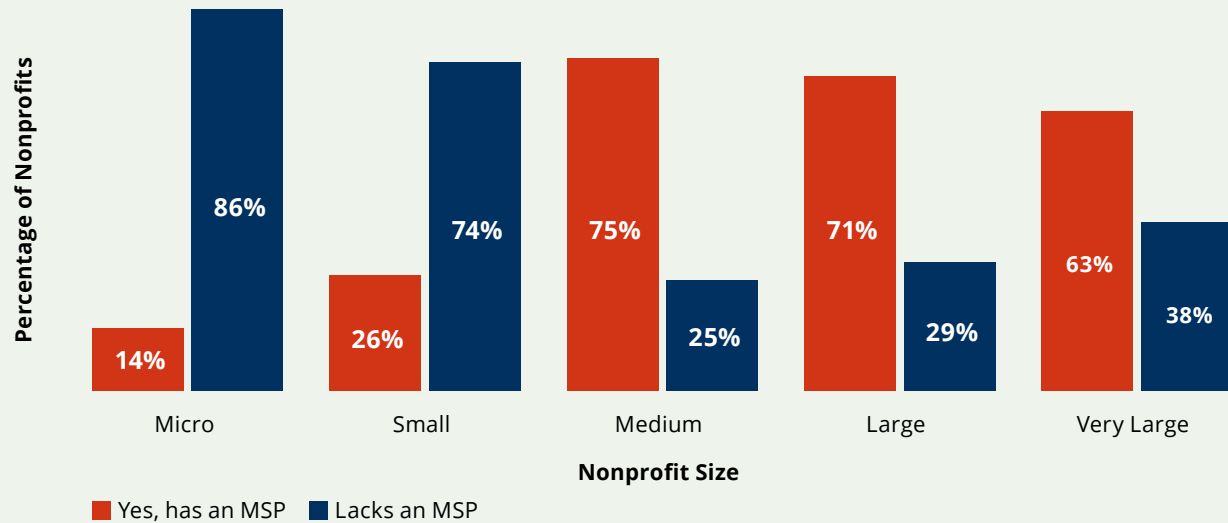
²⁸ Robert Hulshof-Schmidt, *Nonprofit Technology Staffing and Investment Report* (NTEN, 2017).

Smaller nonprofits are less likely to use managed service providers.

Looking at full-time IT staff alone may not provide a complete picture of an organization’s cybersecurity staffing levels. It is possible that nonprofits lean on vendors or otherwise outsource their technology management to managed service providers (MSPs) or managed security service providers (MSSPs) who

specialize in cybersecurity. Unfortunately, this was not the case; over half of nonprofits (56%) did not utilize any MSPs or MSSPs for their technology needs. When sorting the results by size of nonprofits, CLTC learned that smaller nonprofits are far less likely than larger organizations to hire MSPs or MSSPs, at a rate of 14% for micro and 26% for small nonprofits versus 75% for medium and 71% for large nonprofits.

Figure 13: Utilizes an Managed Service Provider (MSP), by Organizational Size



These results demonstrate how cybersecurity inequity perpetuates itself: nonprofits that make little to no investment in IT and cybersecurity often lack relevant in-house expertise to understand where investments are needed and to make use of services like MSPs and MSSP.

This size-based pattern of cyber inequity also applies to resources beyond MSPs and MSSPs. CLTC researchers segmented cybersecurity resource adoption by nonprofit size, examining access to IT staff, MSPs and MSSPs, and dedicated cybersecurity budgets. Across all categories, smaller nonprofits were significantly less likely to have access to these resources. While this finding is not surprising, it is meaningful that smaller nonprofits tend to have the fewest resources to address their cybersecurity risk. This translates into limited staffing and budgets available to build security capacity, thereby increasing their risk.

Why budgets are critical to cybersecurity

A nonprofit’s budget can signal much about the organization’s capacity to make significant changes in investments in cyber. Analyzing technology budget patterns can illuminate not only which resources are available but also the extent to which an organization’s leadership team is invested in bolstering cybersecurity defenses. Moreover, low technology budgets may indicate poorer adoption of cybersecurity controls; for example, an organization might limit large purchases like company-owned laptops and force employees to rely on personal devices. Budgets can also be used to make predictions about the future cybersecurity of an organization. If a budget remains the same or shrinks over time, one can safely predict that large expenditures, such as those needed to add in-house headcount or contract with an MSP, are unlikely.

CLTC analyzed respondents’ budget data in the context of a rapidly intensifying funding crisis for nonprofits in the United States. Rising costs and inflation have led to a 100% increase in nonprofits planning to accelerate layoffs from 2024 to 2025.²⁹ A five-year trend of decreasing donor retention for nonprofits has only compounded this financial uncertainty.

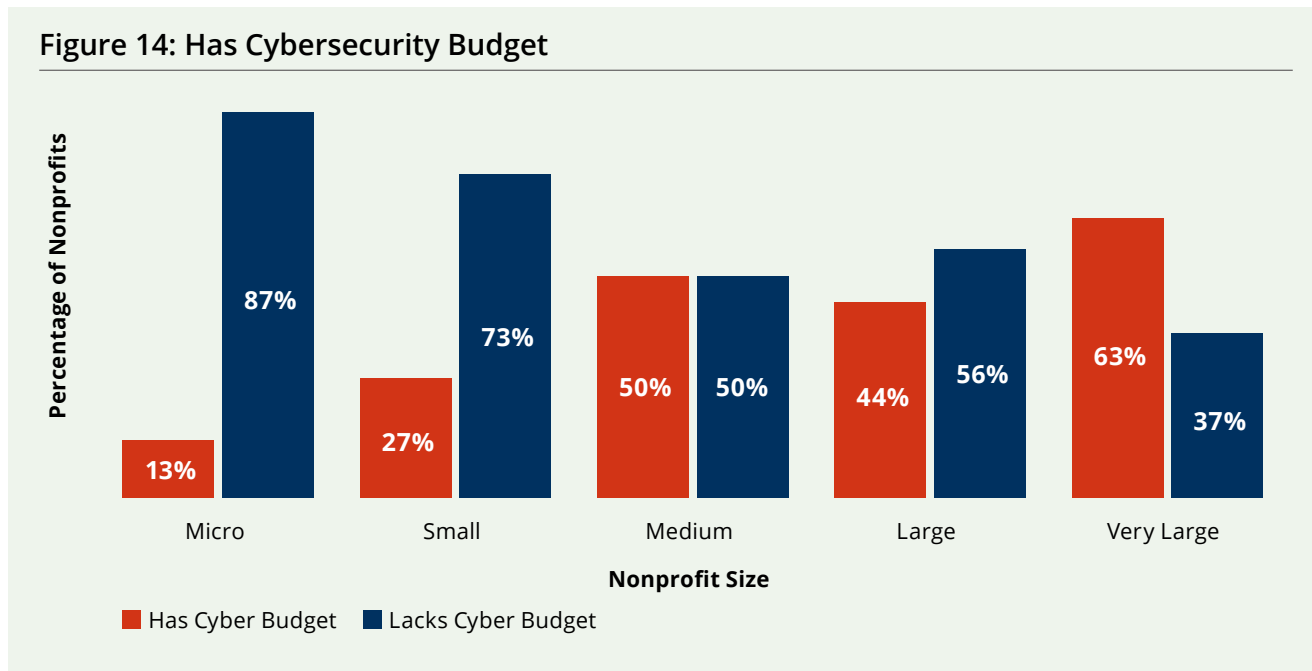
First, CLTC investigated whether nonprofits had a cybersecurity-specific budget in place at all. Most strikingly, 69% of nonprofits did not. Among organizations that did allocate a cyber budget, the average percentage of total budget allocated was 0.83.

For most nonprofits, this placed cybersecurity investments on the backburner, behind other day-to-day technology needs such as internet service, websites, and business-critical applications. But the problem was magnified for smaller nonprofits, which were much less likely to have a cybersecurity budget than larger nonprofits: 87% of micro nonprofits and 73% of small nonprofits lacked a cybersecurity budget, compared to just 37% of large nonprofits.

Survey results show nonprofits are underinvested in cybersecurity and are likely to remain so.

- #1 barrier** to improving cybersecurity is lack of funding
- \$4,311** Avg annual nonprofit spend on IT and cybersecurity
- 69%** of nonprofits did not have cybersecurity-specific budgets

Figure 14: Has Cybersecurity Budget



²⁹ *"The Pressure on Nonprofits Has Never Been Higher—Here's How to Survive What's Coming,"* NonprofitPRO, 23 January 2026.

The average annual cybersecurity expense of surveyed nonprofits was \$4,311. This is lower than the average for small and medium businesses, which typically spend between \$5,000 and \$50,000 per year on cybersecurity.³⁰

CLTC researchers found that senior leadership involvement was associated with a higher likelihood of investing in cybersecurity. Nonprofits with senior leadership actively involved in cybersecurity decision-making were much more likely to allocate a portion of their budget to cybersecurity: 52.3% of organizations with engaged leadership allocated a cybersecurity budget, compared to only 14.7% of organizations without involved leadership.

Lastly, CLTC analyzed whether nonprofits regularly reviewed their cybersecurity budgets. Results showed that over half of nonprofits (54%) had made no changes to their cybersecurity and IT funding in the three years prior. This is a disheartening trend given the relatively low average cybersecurity budget; with escalating cybersecurity threats to nonprofits, nonprofit tech budgets need to be increasing year over year if the organizations are to improve their cybersecurity defenses.

Even small- and medium-sized businesses (SMBs) comparable in size to these nonprofits increase their cybersecurity budgets at much higher rates. Microsoft estimates that 80% of SMBs intend to increase their cybersecurity budgets,³¹ compared to our finding of just 37% of nonprofits that intend to do the same. Of the 37% of nonprofits that increased their IT and cybersecurity budgets in the last three years, the top reasons for this decision were:

- (1) increased awareness of cybersecurity risks,
- (2) leadership's desire to make cybersecurity a higher priority, and
- (3) advice from IT staff or consultants.



When experts describe nonprofits as under-resourced, what they mean is that nonprofits have very small annual expenditures on cybersecurity, often don't separate cybersecurity from their overall budget, and do not have plans to increase their cybersecurity spend moving forward. It is no wonder lack of funding is the #1 barrier to nonprofits improving their cybersecurity, a trend we expect to continue.

30 Val Tsanev, "[Cost of Cybersecurity for Small Businesses: What You Need to Know](#)," Execweb, 21 April 2025.

31 Scott Woodgate, "7 Cybersecurity Trends and Tips for Small and Medium Businesses to Stay Protected," Microsoft Security (blog), 31 October 2024.

4. The Digital Isolation of Nonprofits

Finding #4:

Nonprofits struggle to prioritize cybersecurity until an incident occurs and lack the knowledge to make necessary improvements in the aftermath.

Prioritizing cybersecurity is difficult for nonprofits, especially before a cybersecurity incident occurs.

Nonprofits ranked “difficulty prioritizing cybersecurity over competing objectives” as the second most important barrier to improving cybersecurity. This challenge is neither unexpected nor unique to the nonprofit sector. For-profit companies also struggle to prioritize cybersecurity—an abstract risk mitigation for seemingly unlikely incidents—over more immediate operational needs.³² What is more distinctive about nonprofits, however, is the trade-off they face between investing in cybersecurity and delivering on their core service missions. With such finite resources, strengthening cybersecurity can mean diverting funds, time, or staff away from programs that directly support beneficiaries. In an interview with CLTC, one nonprofit shared that even if additional funding became available, there were “several other staffing needs” that were “more pressing” and “multiple other hires that we would make before we would turn to an IT person.” Similar tensions exist in other resource-constrained public interest sectors, such as healthcare. For example, it is difficult for a rural hospital to justify a large expenditure of time or money on cybersecurity when that same investment could add another hospital bed.

This phenomenon is especially pronounced among nonprofits that have not yet experienced a cyber incident. Many nonprofits see cybersecurity as an optional and intangible investment until they experience a cyberattack that makes the risks concrete. Across interviews, cyberattacks were catalysts for change within nonprofit organizations, serving as “aha” moments that prompted leadership to take their cyber

risk more seriously and begin allocating time and budget toward security improvements.

Take, for instance, a Washington-based addiction and homeless services nonprofit CLTC interviewed. This organization experienced a business email compromise incident that led to an attempted fraudulent bank transfer, nearly resulting in the withdrawal of most of its funds. The program director and co-founder personally led the investigation and response effort, as the organization had no IT or cybersecurity staff and no established procedures for seeking assistance from a cybersecurity consultant. “I lost a lot of sleep because we had to get that money back to make payroll,” he recalled. The nonprofit contacted the FBI Financial Crimes Help Line, which directed them to the appropriate representative at their bank.

In response to the incident, the nonprofit made several security improvements. They changed all major organizational platform passwords, enabled MFA on their accounts, moved their passwords to an offline, password-protected spreadsheet of credentials, and required the use of a VPN to access the internet for all employees. They are also considering the possibility of utilizing volunteer help to migrate the organization to a single sign-on solution with MFA. It took the immediate threat of a cyber incident to push the nonprofit’s leadership to prioritize cybersecurity more effectively in the short and medium term.

Another nonprofit we interviewed shared a similar story. After losing a \$300,000 payment due to email fraud, the nonprofit implemented MFA for all employee email accounts, improved security of firewalls, and increased staff cybersecurity training.

³² “Organizations Seldom Prioritize Cybersecurity Over Business Outcomes,” Help Net Security, 5 November 2021.

In written survey responses, other nonprofits reported implementing the same kinds of improvements, plus a few others, including new security procedures for auditing internal systems for vulnerabilities and monitoring transactions and bank accounts more closely.

Many of these improvements, however, are led by staff without formal cybersecurity expertise, which can produce potentially suboptimal practices. For example, one nonprofit nearly lost all of its funds after an attacker accessed an executive director’s email and found a spreadsheet containing all of the organization’s passwords, including their bank account credentials. In response, the nonprofit changed all the passwords but maintained a password spreadsheet—which is now password-protected and prohibited from being emailed—but stored it on a shared flash drive. Albeit well-intentioned, this new approach relies on shared credentials and lacks the safeguards of a dedicated password manager.

Many nonprofits lack the knowledge to make appropriate improvements in their cybersecurity defenses.

CLTC sought to understand whether organizations that did have funding were equipped to make the necessary improvements in their cyber defenses. Would they know which tools they needed, if any, to implement basic cybersecurity controls?

Indeed, CLTC researchers found the third most significant barrier to cybersecurity that nonprofits identified was “knowledge of what to improve.” They were particularly uncertain about what to purchase. When asked which cybersecurity and software tools were most needed, the most popular response was “We are unsure what we need.”

No single tool stood out as the top cybersecurity need for nonprofits. Respondents ranked data recovery and backup tools as their highest need, followed by password managers, email phishing detection tools, and work devices.

Most Desired Cybersecurity Software and Tools Among Nonprofits

- 1. “We are unsure what we need.”**
- 2. Data backup and recovery tools**
- 3. Password managers**
- 4. Email phishing detection tools**
- 5. Work devices (e.g., laptops, phones)**

This lack of knowledge may be influenced by civil society’s relative isolation from the cybersecurity field compared to the private sector. For one, nonprofits lack strong, longstanding membership organizations centered on cybersecurity. Large information sharing associations, which collect, analyze, and disseminate actionable cybersecurity and physical threat information to their members, have existed for decades, including the E-ISAC (electricity), FS-ISAC (financial services), and Health-ISAC (healthcare). Nonprofits had no comparable association until 2017, when NGO-ISAC was founded, followed by NetHope’s Global Humanitarian ISAC in 2022.

Nonprofits are similarly excluded from grant programs that provide funding for projects shoring up cyber defenses of local communities, such as the landmark State and Local Cybersecurity Grant Program (SLCGP) and the Tribal Cybersecurity Grant Program (TGCP), which only provided funding to state, local, tribal, and territorial (SLTT) governments.³³ This exclusion persists despite the fact that some direct-service nonprofits function as extensions of SLTT governments by fulfilling contracts to deliver social services. For example, New York City’s street outreach

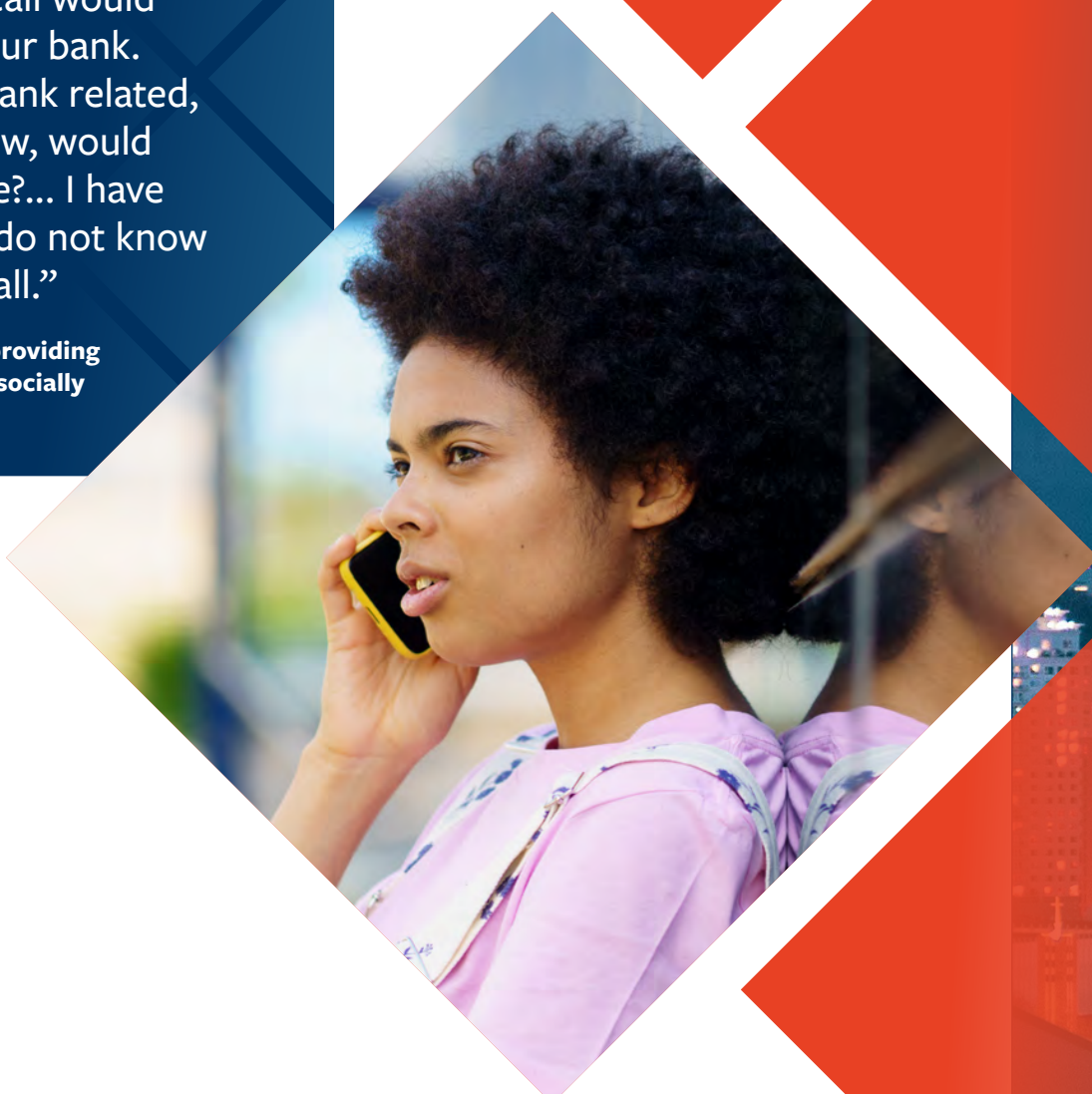
³³ [State and Local Cybersecurity Grant Program Frequently Asked Questions](#), America’s Cyber Defense Agency, [Tribal Cybersecurity Grant Program](#), America’s Cyber Defense Agency.

to unhoused individuals on behalf of the Department of Homeless Services is conducted by nonprofits, not full-time city employees.³⁴

This isolation has real implications for the resilience of nonprofits to cyberattacks. Less community means less shared knowledge, less preparedness, and poorer incident response and recovery. One nonprofit shared in an interview that they wouldn't know whom to contact in the event of a cyber incident:

“I think our first call would probably be to our bank. But if it wasn't bank related, yeah, I don't know, would we call the police?... I have no idea. No, we do not know who we would call.”

Washington nonprofit providing support and funding to socially impactful startups



34 [“Street Outreach,”](#) NYC Department of Homeless Services.

Comparing Washington and San Francisco Findings

After analyzing the results from the CyberCAN Washington survey, CLTC revisited the results from the first iteration of this survey project and report for the City and County of San Francisco to assess whether nonprofits across San Francisco and Washington State faced similar cybersecurity challenges, and where key differences could be found. This cross-region comparison also provides clues as to whether the findings might be generalizable across the U.S., or whether nonprofits vary significantly in cyber protections depending on their area of residence.

Both San Francisco and Washington studies point to the same cycle: organizations with the fewest resources are also the least likely to invest in cybersecurity, perpetuating cybersecurity inequity across the nonprofit sector.

Nonprofits faced similar threats across San Francisco and Washington State.

This CyberCAN Washington study corroborated the the CyberCAN San Francisco study's core conclusion that phishing is the most common cyber threat facing nonprofits. In both surveys, respondents ranked phishing first, followed by BEC and then financial fraud third—preserving the same rank order across every major attack category. This consistency suggests that the threat landscape nonprofits face is not shaped by local conditions but rather reflects a sector-wide vulnerability pattern that holds regardless of geography.

There was high consistency in reported incident rates across the two studies, with nearly identical percentages across most categories. For example, 33% of surveyed nonprofits in Washington State and 32% in San Francisco had experienced BEC, and results from Washington State on other attacks, such as credit card or bank

account fraud, gift card scams, and ransomware, were all within 5% of the results from San Francisco. There were a few small differences between the attack data from Washington State and San Francisco. Washington nonprofits reported lower phishing rates (56% vs. 71%) and lower physical break-in and document theft rates when compared to San Francisco (5% to 15%), but substantially higher incidences of data loss / leak (14% vs. 9%). This gap likely reflects differences in sample size, geography, and how incidents were defined and reported across the two studies rather than a genuine discrepancy in threat exposure. Any cybersecurity strategy aimed at nonprofits should treat phishing, BEC, and financial fraud as the primary threats to address.

IT understaffing is common across Washington State and San Francisco, with a clearer divide between large and small nonprofits.

The CyberCAN San Francisco study's concern about nonprofit IT understaffing was also substantiated by this CyberCAN Washington. Both studies show that the majority of nonprofits have no dedicated IT staff, with 54% in San Francisco and 63.9% in Washington reporting no IT personnel whatsoever. The drop-off in IT staff for those nonprofits that had any is steep in both studies: San Francisco saw only 21% reporting one IT staff member and only 10% reporting two, while Washington State followed a nearly identical pattern, with 19.6% reporting one staff member and just 4% reporting two. Very few nonprofits in either study reported three or more IT staff, and those that did represented a small minority in both populations. The identical IT-to-staff ratios of 1:96 in both Washington State and San Francisco further confirm that this is a structural, sector-wide condition rather than a regional anomaly.

The key difference between staffing in Washington State and San Francisco was in the share of nonprofits reporting zero dedicated IT staff, with 54% in San Francisco versus 64.4% in Washington. This disparity suggests the staffing crisis may be more acute outside major metropolitan areas where tech talent is more concentrated. The Washington study's finding that 65.3% of nonprofits have someone informally absorbing IT

duties reinforces the San Francisco study's narrative concern that cybersecurity responsibilities are quietly falling on undertrained staff.

The two studies diverge more sharply in MSP or MSSP adoption. The San Francisco study reported 40% of nonprofits using MSPs or MSSPs, with a notable 24% indicating they were unsure. Washington reported a somewhat higher adoption rate of 44%, with no comparable uncertainty category. While the overall usage figures are reasonably close, this Washington State report's organizational size breakdown revealed that micro and small nonprofits used MSPs or MSSPs at far lower rates than larger organizations, reinforcing the San Francisco study noteworthy finding that the nonprofits most in need of outside support are the least likely to access it. Both studies point to the same cycle: organizations with the fewest internal resources are also the least likely to supplement them externally, creating cybersecurity inequity across the sector.

MFA adoption alone did not correlate with fewer incidents.

The Washington study's ranked obstacle data validated the San Francisco study's finding that funding and knowledge gaps were the primary barriers to stronger cybersecurity controls, with the two studies independently identifying the same top two barriers despite using different measurement approaches. The Washington State study's MFA incident data introduced an important nuance: nonprofits with MFA experienced incidents at a rate of 44%, only marginally lower than the 42% rate among those without it, which complicates the assumption that MFA adoption alone produces meaningfully better outcomes.

Only 10% of Washington nonprofits reported not using MFA for any platform whatsoever, a slight improvement compared to the 16% that reported no MFA use in the San Francisco study. This result suggests that Washington nonprofits have begun adopting MFA as a basic security control.

This narrow gap likely reflects the reality that isolated control adoption does not provide the same protection as a comprehensive strategy. When funding and knowledge are the binding constraints, organizations

tend to implement whatever is most visible or easiest rather than what is most strategically effective, producing the appearance of progress without proportionate reductions in risk.

Nonprofit funding is geography-dependent, except for foundations and federal funding sources.

The Washington State study confirms our findings in the San Francisco study that funding and prioritization are the two dominant obstacles to cybersecurity investment. Foundation-based funding is the most consistent data point across both studies, with 84% of San Francisco nonprofits and 80.9% of Washington nonprofits relying on it, suggesting foundations are a near-universal funding source for the sector regardless of geography. Both populations rely heavily on city and local government grants, but more so in San Francisco, at 91% compared to 69.7% in Washington. This disparity is particularly relevant given the San Francisco study's emphasis on overhead caps as a structural barrier to cybersecurity spending.

Federal grant reliance is closely aligned across the two studies, at 46% and 43.8%, respectively, suggesting that federal funding dynamics and any associated compliance requirements are relevant to both populations. Given that the studies differ in focus, with one being a city-level survey and one being a state-level survey, this finding helps explain the increase in state funding sources in Washington and, inversely, the increase in city/local government funding in San Francisco. The broad scope of nonprofits across an entire state also results in a wider array of individual donor contributions, considering both urban and rural areas. On the other hand, nonprofits in San Francisco, with its concentration of economic and technology giants, would see higher average individual donor rates of 84%, compared to Washington's 67.4%.



Recommendations

These recommendations are developed by CLTC alone based on our analysis of the survey and nonprofit interviews.

They are presented in order of increasing expected cost and operational burden required for implementation, beginning with actions nonprofits can take directly and progressing to coordinated government-led interventions.

1

Nonprofits should reduce the amount of sensitive data they collect.

2

City and county governments should play a coordinating role in connecting local nonprofits to cybersecurity resources that align with their budgets and needs.

3

The State of Washington should establish a short-term working group on nonprofit cybersecurity to define and operationalize local government coordination.

4

The State of Washington should include nonprofits in the full scope of support provided by centralized resources, such as the Washington Volunteer Cybersecurity Incident Response Team (CIRT).

5

The State of Washington and well-resourced city and county governments should offer shared cybersecurity tools and services to nonprofits.

6

Washington State should invest in expanding and strengthening supportive programs tailored to the cybersecurity needs of nonprofits.

1 Nonprofits should reduce the amount of sensitive data they collect.

Nonprofits are at heightened risk of cyberattacks and their lean budgets and limited in-house expertise can increase that risk. But one easy solution that does not require cybersecurity expertise can dramatically lower the chance of leaking sensitive data: not collecting such data whenever possible.

While much of the client data collected by nonprofits is stored to remain in compliance with grant funding requirements, some is gathered simply to track and stay connected with their clients and donors. Nonprofits should reassess what information mission critical or required, versus what is merely useful, and limit their data collection accordingly. Nonprofit leaders should work with their teams to decrease or eliminate the collection of highly sensitive personally identifiable information (PII) from their workflows and delete historical data. They should pay particular attention to financial information, health information, location information, and information relating to protected classes, such as race, gender, ethnicity, religion, or sexual orientation.

In cases where nonprofits are unable to reduce the information being collected, they must acknowledge the risks of data breaches and commit to implementing essential, effective cybersecurity controls to protect this information from unauthorized access. Nonprofits unable to deploy these interventions on their own can work closely with cyber volunteering organizations that offer free cybersecurity consulting and support, such as the Eastern Washington University Cybersecurity Clinic³⁵ and the CyberPeace Builders Program (CBP)³⁶, developed by the Cyber Peace Institute.

2 City and county governments should play a coordinating role in connecting local nonprofits to cybersecurity resources that align with their budgets and needs.

Local governments are well positioned to serve as intermediaries that help nonprofits access cybersecurity support before and after cyber incidents. In practice, this coordination role can include directing nonprofits to resources, such as cyber volunteering organizations offering pro bono cybersecurity services (e.g., incident response, security assessments, or technical consulting) and lists of MSPs and MSSPs that specialize in assisting nonprofits. Local governments can also pass along practical, accessible guidance on baseline security practices and post-incident steps and can connect nonprofits to existing cybersecurity and technology grant programs that fund security improvements.

While each governmental entity may be organized differently, interviews conducted by CLTC suggest that human services departments and digital equity departments, in coordination with local IT departments, may be best positioned to carry out this role. These departments interact frequently with nonprofits that receive government grants and contracts—often communicating monthly, if not weekly—and already function as support hubs that connect service providers to operational resources. Expanding this function to include sharing cybersecurity resources would be a modest extension of their existing responsibilities. Several interviewees also noted that nonprofits are sometimes required to notify these departments when breaches involve resident data, indicating that these offices are already a point of contact when incidents occur.

35 Eastern Washington University. “[EWU Lands \\$1 Million Google Grant for Cybersecurity Clinic](#).” June 4, 2024

36 CyberPeace Institute. “[CyberPeace Builders](#).”

3 **The State of Washington should establish a short-term working group on nonprofit cybersecurity to define and operationalize local government coordination.**

While local governments are well positioned to play a coordinating role, interviews revealed that most city and county personnel have not considered the cybersecurity risks associated with nonprofits receiving public funding and are often unaware of incidents affecting them. Several respondents also expressed uncertainty about the scope of their responsibilities and requested clearer guidance from the Washington state government on how to support nonprofits in this area.

A state-led working group could help operationalize this coordination model by defining the role of local governments and curating the resources needed to support it. State-level leadership on this topic is needed given existing capacity constraints. Human services and digital equity departments, while best positioned to interface with nonprofits, generally lack the staffing and bandwidth to do so. Washington state agencies can fill this gap by leading the establishment of a dedicated workgroup and overseeing the curation of resources, enabling local governments to implement coordination without taking on significant new operational burdens.

We recommend that the state government involve WaTech in this project, which aligns with Washington's broader mission to advance cybersecurity across the state's public-sector ecosystem, including county, city, and tribal governments and public-benefit nonprofits. By equipping local governments with clear guidance and vetted resources, Washington can help build a scalable, statewide model for strengthening nonprofit cybersecurity.

4 **The State of Washington should include nonprofits in the full scope of support provided by centralized resources, such as the Washington Volunteer Cybersecurity Incident Response Team (CIRT).**

Washington is leading the nation by starting up a cost-effective cyber defense program: the Washington Cyber Incident Response Team (WA CIRT), housed in the Washington Emergency Management Division. This program should be fully funded by the State of Washington so that it can provide pro bono cybersecurity services to organizations that otherwise cannot afford them, including nonprofits.

Through WA CIRT, skilled volunteers credentialed under the state's Emergency Worker Program will help Washington's community organizations detect, contain, and recover from cyber incidents. The team will also help with proactive trainings and other community-building programs for under-resourced organizations like nonprofits. The team is in its infancy, but the model of volunteer response corps has been proven in other regions; six states—Louisiana,³⁷ Maryland,³⁸ Michigan,³⁹ Ohio,⁴⁰ Texas,⁴¹ and Wisconsin⁴²—have active cyber volunteer corps programs,⁴³ with over 900 volunteers spread across them.⁴⁴ WA CIRT can promote workforce development while filling critical gaps in cybersecurity preparedness and response, and a fully funded and authorized WA CIRT has the potential to address many of the areas of highest risk raised in this report. More information on volunteer cyber corps programs can be found in CLTC's 2026 guidebook on whole-of-state cybersecurity.⁴⁵

37 [State Guard—Louisiana National Guard](#).

38 [Maryland Defense Force](#).

39 [Michigan Cyber Civilian Corps \(MiC3\)](#).

40 [OhCR—Ohio Cyber Reserve](#).

41 [Texas Volunteer Incident Response Team \(VIRT\)](#), Texas Department of Information Resources.

42 Wisconsin Cyber Response Team, Wisconsin Emergency Management.

43 Though not a formal cyber corps program, California maintains a Cybersecurity Integration Center comprising personnel from various state agencies and tasked with sharing threat intelligence and providing incident response services.

44 Michael Razeed, "[Civilian Cyber Corps: A Model Law for States](#)," New America, 26 September 2024.

45 CLTC, "Save Money, Build Talent, and Defend Communities: A Whole-of-State Cybersecurity Guidebook," 2026.

5 The State of Washington and well-resourced city and county governments should offer shared cybersecurity tools and services to nonprofits.

Washington’s nonprofits have limited in-house expertise and lean budgets. The Washington state government, together with well-resourced cities and counties, should leverage their purchasing power to assist nonprofits in acquiring critical cybersecurity tools and services while sparing them high costs and burdensome procurement processes.

Nonprofits should first ensure they are fully leveraging existing no-cost cybersecurity capabilities embedded in their digital tools, where available. Tools such as Google Workspace for Nonprofits and Microsoft 365 for Nonprofits already provide some security protections, including email filtering, endpoint management, and identity controls. However, these baseline offerings are often insufficient on their own, and there remains a need for additional support, particularly for more advanced protections and ongoing management.

Government digital equity departments already invest in the public good of connecting everyone to the internet; it is commonsense to expand this mission to include basic cybersecurity protections on the internet. For example, cities and states work with internet service providers to offer lower-cost broadband service to qualifying residents. A similar mechanism could be successful in expanding cyber tools (e.g., firewalls, filtering, DDoS mitigation, and endpoint protection) and services (e.g., managed IT or managed cybersecurity service providers). As an example, the New York State Cyber Shared Services Program provides critical tools at no cost to eligible local governments, including endpoint detection and response, attack surface management, and security information and event management.

6 The State of Washington should invest in expanding and strengthening supportive programs tailored to the cybersecurity needs of nonprofits.

Given nonprofits’ role in delivering public services and managing sensitive data on Washington residents, the state has a vested interest in ensuring these organizations are not left more vulnerable as federal support declines. In May 2025, the Trump administration rescinded the Digital Equity Act and its grant programs, including nearly \$16 million awarded to Washington. These funds were intended to support a Broadband Cybersecurity Literacy Program to promote digital literacy and deliver advanced cybersecurity training across the state. In July 2025, the Washington Department of Commerce’s Digital Navigator Program—which leveraged trusted community partners to deliver outreach, in-person training, and tools and educational resources to support technology adoption—was defunded and discontinued due to grant program mismanagement by the Department, which was investigated and reported on by the Washington State Auditor.⁴⁶ The loss and shortcomings of these programs has created stark gaps in access to cybersecurity training and support.

To address these gaps, Washington can draw on proven models at the federal, state, and local levels while recognizing the constraints posed by a tight budget environment. For example, leaders can ramp, improve, and adapt elements of the Digital Navigator Program to deliver cybersecurity awareness, training, and support to nonprofits through trusted intermediaries like cyber volunteering organizations. In parallel, the state can establish dedicated grant funding to help nonprofits invest in cybersecurity capacity, tools, and services. One model is the Federal Emergency Management Agency’s (FEMA’s) Nonprofit Security Grant Program, which provides funding support of up to \$200,000 for physical and cyber security enhancements to nonprofit organizations at high risk of terrorist or other extremist attacks. Another model is the U.S. Department of Homeland Security’s State and Local Cybersecurity Grant Program (SLCGP), which was one of the most successful in the nation at allocating funding to local governments to address cybersecurity challenges. While it was reauthorized by Congress through January 30, 2026, it was not funded and has since expired. Its future now remains uncertain. Programs such as these would expand access to cybersecurity support and could strengthen the resilience of Washington’s nonprofits and public services.

⁴⁶ Office of the Washington State Auditor Pat McCarthy, “*Performance Audit: Assessing the Department of Commerce’s Management of the Digital Navigator Program*,” 27 January 2026.



Conclusion and Future Research



It is not unknown, nor surprising, that nonprofits face a significant uphill battle to reach a basic level of cybersecurity defenses. But more empirical research initiatives like CyberCAN Washington and San Francisco are needed to shift the narrative from one of hopelessness to one of targeted action. From CLTC's survey, we know of some Washington-specific findings that can be rectified and will be of interest to policymakers both local and national.

CLTC has shown that nonprofits frequently experience cyberattacks that disrupt operations, cause financial losses, and expose sensitive data, and that over three-quarters of nonprofits had experienced at least one cyberattack in the last three years. Our analysis of nonprofits' implementation of cybersecurity controls showed that they collect sensitive information and have limited adoption of the most effective cybersecurity controls, and that nonprofits that stored "highly sensitive" PII were more likely to experience a cyberattack than other nonprofits. We found that nonprofits do not have the capacity to invest in cybersecurity due to insurmountable staffing and budget constraints, trends that are very likely to continue. Lastly, we demonstrated that small nonprofits struggle to prioritize cybersecurity until an incident occurs and lack the knowledge to make necessary improvements in the aftermath.

There are concrete actions that can be taken to improve nonprofit cybersecurity, and CLTC put forth recommendations for state, city, and county governments to aid nonprofits. CLTC also calls on nonprofit leaders to take action by reevaluating their data collection in light of their heightened cyber risk and lower defenses.

As CLTC continues to research nonprofit cybersecurity and advocate for shifting the burden away from nonprofit employees, we are heartened by the stalwart support of many local government partners from the City and County of San Francisco, the City of Seattle, and the State of Washington. These leading public servants understand the value nonprofits provide to residents and the urgency with which they must act to defend these same organizations from digital harm. CLTC thanks these partners for their leadership and commitment to these causes and hopes they pave the way for even more regional support for nonprofits across the United States.

CLTC hopes to see the CyberCAN survey administered in more regions in the U.S. so that researchers can compare findings. We would be glad to provide our methodology and analysis advice to academic teams interested in surveying their locality. Moreover, CLTC is always willing to connect interested parties directly with active cyber volunteering organizations offering pro bono cybersecurity services to nonprofits.



Acknowledgments

This research would not have been possible without the generous support of Okta for Good, whose philanthropic efforts help nonprofits worldwide build their cyber resilience and expand their mission impact. Their support for academic and applied cybersecurity research enabled CLTC to launch the CyberCAN program in San Francisco in 2023 and begin this work in Washington State in 2025.

CLTC also extends its sincere gratitude to WaTech for its partnership and for providing a home for this research. The agency's commitment to protecting nonprofit organizations from cyberattacks in Washington State is both notable and appreciated. We thank Washington State Chief Information Officer Bill Kehoe for his department's leadership on this topic and for platforming this effort, as well as Zack Hudgins for his steadfast support and sage advice throughout this project.

In addition, we extend our thanks to the numerous state, county, and city and government departments and the many nonprofits that generously helped distribute our survey and participated in interviews. Your time and perspectives were invaluable in strengthening our analysis and shaping our recommendations.

We also thank Indiana University's Center for Applied Cybersecurity Research and its executive director, Craig Jackson, for allowing us to draw from and model after aspects of the CyberTrack methodology. CyberTrack's work is groundbreaking and continues to make a meaningful impact for public interest cybersecurity organizations throughout Indiana, and your guidance helped inform our approach. We also appreciate our partners at NGO-ISAC for reviewing our survey instrument and for helping ensure it was clear and accessible for nonprofit audiences.

Finally, we thank the City of Seattle's IT department for the opportunity to translate this research into action for the local nonprofit community by hosting the report launch and a nonprofit cybersecurity resource fair at Seattle City Hall. In particular, we are grateful to City Chief Information Security Officer Jake Hammock, Megan Erb, and Kristeena Gargia for their generosity, collaboration, and support.





CLTC
Center for Long-Term
Cybersecurity

WaTech
Washington Technology Solutions