CLTC
Center for Long-Term Cybersecurity
UC Berkeley

CYBER RESILIENCE CORPS
USA

CyberPeace Institute

# The Roadmap to Community Cyber Defense

## A Path Forward from The Cyber Resilience Corps

Sarah Powazek, Grace Menna,
The Cyber Resilience Corps

June 17, 2025

# Table of Contents

# Executive Summary

Today, cybersecurity is a lonely road for many. Community organizations — nonprofits, rural hospitals, schools, local utilities, counties, municipalities, and small businesses — are vital to delivering essential services to the public, but they are often the least prepared to protect themselves from cyberattacks and are often wholly responsible for their own defense. Hands-on support from a broad coalition of groups is needed to provide a safety net that strengthens these organizations' cyber defenses, ensuring they can continue their vital work securely and without disruption.

This ambitious report marks the culmination of the first year of operations of the Cyber Resilience Corps, a dedicated group of practitioners working to provide digital security assistance to community organizations. Co-chaired by the UC Berkeley Center for Long-Term Cybersecurity (CLTC) and the CyberPeace Institute, the Cyber Resilience Corps brings together cyber volunteering leaders, private-sector partners, experts, and community leaders.

To develop the report, we critically examined the structural barriers that lead to cyber insecurity among community organizations, and we charted a path forward to mobilize more cyber civil defenders and protect a growing number of community organizations from cyber attacks.

As detailed in the report, we first propose a "co-responsibility model" for cybersecurity that details what cyber responsibilities community organizations can reasonably be expected to shoulder and what duties should be shifted towards other, more capable actors.

We then propose an "on-ramp" to address immediate gaps in services, with nine specific recommendations to rapidly assist our local schools, cities, nonprofits, and utilities across three lines of effort: 1) maturing cyber volunteering programs, 2) expanding cyber volunteering programs, and 3) enhancing continuity of service after volunteer engagements conclude.

We also propose a long-term "destination" that the cybersecurity industry must work toward in order to shift the burden away from community organizations. These interventions include 1) companies simplifying cybersecurity for non-experts, 2) states creating shared services for community organizations, and 3) embedding cyber knowledge in our communities.

Finally, we include a guidebook for state leaders to invest in their local cyber support ecosystems by establishing and supporting programs like cyber clinics, civilian cyber corps, and nonprofit cyber volunteering groups.

Cybersecurity support for community organizations cannot wait for long-term change; we all need a roadmap to show us the way forward. There may be hazards, but if enough people pull over to lend a hand, all organizations can get on the road to cyber resilience together.

# About the Cyber Resilience Corps

## Taking up the Gauntlet from CISA and Cyber Civil Defense

Coined by philanthropist Craig Newmark, founder of the Cyber Civil Defense Initiative, the term “cyber civil defense” has come to describe the incredible work of a swath of organizations working to defend communities in the United States from cyber attacks, including by sharing threat intelligence, developing toolkits, educating everyday Americans, and providing hands-on assistance.

CLTC has been a long-time organizer and provider of cyber civil defense services, and this latter category is where our work is squarely situated: we founded and co-chair the Consortium of Cybersecurity Clinics,[1] a network of over 50 university and college-based clinics around the world that train students to provide free cybersecurity assistance to local schools, cities, hospitals, and nonprofits.

Through CLTC’s work stewarding clinics worldwide, our team has worked closely with other grantees of Craig Newmark Philanthropies in the Cyber Civil Defense Initiative, as well as with the Cybersecurity and Infrastructure Security Agency (CISA) High-Risk Communities Protection Initiative,[2] a 2024 program established by CISA’s Joint Cyber Defense Collaborative (JCDC) to centralize resources for communities at heightened risk of cyber attacks. Emerging from both of these groups was one core theme: community organizations as a whole are falling through the cracks, and current efforts are not enough to help them protect themselves online.

In November 2024, CLTC partnered with the CyberPeace Institute to found the Cyber Resilience Corps, with the goals to: 1) use cyber volunteering to create a safety net for as many organizations as possible; and 2) drive long-term solutions to a system that currently fails the organizations that power our communities, including nonprofits, rural hospitals, schools, municipalities, and small businesses.

The Cyber Resilience Corps unites and strengthens volunteer efforts to deliver real, hands-on cybersecurity support where it is needed most. Until now, the diverse organizations that deliver volunteer cybersecurity assistance have functioned mainly in siloes, with little coordination or collaboration, limiting their scale and impact. Bringing together these service providers and the organizations they benefit has helped us understand the current system for community organizations and chart a path forward that works for entire communities.

# Convening the Cyber Resilience Corps

In January 2025, CLTC and CyberPeace Institute hosted the Cyber Resilience Corps Working Group, composed of over 30 individuals,[3] to tackle the challenge of creating a roadmap for the cyber defense of community organizations. This working group purposely included a wide range of stakeholders — including cyber-defense toolmakers and providers, helplines, policymakers, industry leaders, investors, and representatives from coordinating bodies — to ensure a diversity of perspectives and depth of understanding as we establish and share best practices, address service gaps, and strengthen nationwide collaboration.

The Cyber Resilience Corps met for three two-hour sessions during the first half of 2025. Each session broke participants into two or three breakout groups, with members of CLTC and the CyberPeace Institute co-leading the discussions. The group discussed key challenges facing community organizations and recommendations for immediate and long-term action to build a safety net for community organizations.

The third and final session, held in May 2025, asked participants to provide feedback on an initial draft of the recommendations found in this report. While not every member agrees with every recommendation, the report represents many of the themes about which the group achieved consensus. Because many members work in high-risk areas of cybersecurity, only those individuals who have agreed to be publicly acknowledged are listed at the end of this paper.

# The Status Quo and Its Consequences

## Quantifying the Threat to Community Organizations

The cyber threat to community organizations is widely known and frequently acknowledged, but to date, it has been poorly proven.

Cybersecurity has a data problem: none of the experts consulted for this report was aware of nationwide data quantifying the scale of this issue outside of individual corporate reports, which are limited by the information that can be collected from their own customer bases and often focus on trends. Existing non-corporate research is largely focused on mapping the attack surfaces of particular sectors or subsectors and tends to focus on proxies for attack surfaces, such as open ports, to extrapolate to overall cyber maturity (see figure below). Without mandatory and consistent cyberattack reporting to a single entity, the decentralized nature of cybersecurity data will continue to cloud the true scale of the threats facing our communities.

We attempt to centralize the most compelling statistics on community cybersecurity here. We also present a few key examples of pernicious attacks to illustrate the dangers that community organizations face on their own.

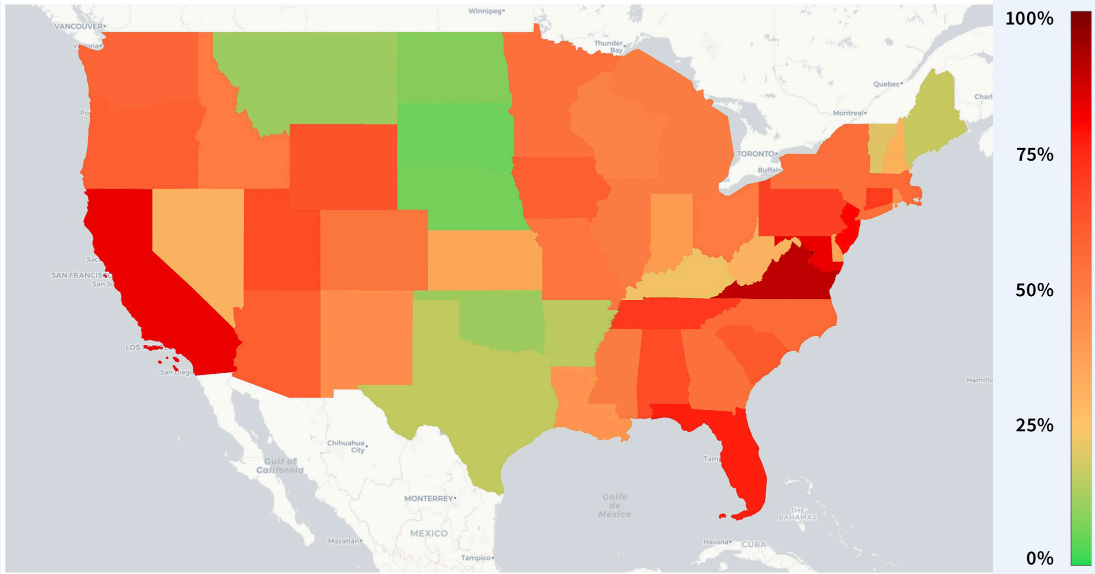


**Figure 1:**

Percentage of counties within U.S. states that are potentially susceptible to insecure authorization.[4] Such data represents a useful but imperfect proxy for the cyber risks facing community organizations.

Source: Harry, Charles, et al. "Measuring the Size and Severity of the Integrated Cyber Attack Surface across US County Governments." Journal of Cybersecurity, vol. 11, no. 1, Jan. 2025, p. tyae032. Silverchair. Licensed under CC BY-NC-ND.

## Threat Data

**Healthcare:**
In 2024, 67% of global healthcare facilities were hit by ransomware, jeopardizing patient care in underserved areas. On average, 58% of computers in healthcare organizations are impacted by a ransomware attack.[5]

**Schools:**
The global education sector experienced a 69% increase in ransomware incidents during the first quarter of 2025 compared to the same period in 2024, with 81 incidents reported, compared to 48 in 2024.[6]

**Nonprofits:**
According to CPI's CyberPeace Tracer,[7] 121 civil society organizations faced over 43,000 incidents between 2023 and 2025.

**State and local governments:**
According to Sophos,[8] 34% of state and local governments experienced a ransomware attack in 2024.

**Utilities:**
Between January-August 2024, 1,162 cyberattacks on U.S. utilities were documented, a 70% increase compared with the same period in the prior year.[9]

## Pernicious Cyber Attacks

**Food insecurity:**
As of 2024, cyber criminals had stolen over $69 million in EBT food stamp accounts from over 143,000 low-income households.[10] As a result, 53% of EBT theft victims were forced to skip meals, and 44% had to borrow money or go into debt.[11]

**Health disruptions:**
In January 2025, New York Blood Center Enterprises, which collects approximately 4,000 units of blood products daily and serves more than 400 hospitals across dozens of states, was a victim of a ransomware attack[12] during an emergency period of critically low blood availability. The ransomware attack resulted in the cancellation of 17 blood drives and significantly impacted the already low supply of types O and B blood.

**School cancellations and threats to children:**
In January 2023, Tucson Unified School District, the second-largest school district in Arizona with approximately 42,000 students, was crippled by a ransomware attack, forcing the closure of schools for two weeks.[13] Personal information of some employees and students was leaked onto the dark web, where it was available for sale to the highest bidder, exposing minors to harassment and identity theft.

**25%**

**of cybercrimes were reported globally in**

**2024**

Many cyber attacks are not reported; less than 25% of cybercrimes were reported globally in 2024, according to Cybersecurity Ventures.[14] Without visibility into data on nationwide attacks, we expect that the statistics above represent only a fraction of the cyber threats facing our communities.

# The Cyber Poverty Line Status Quo

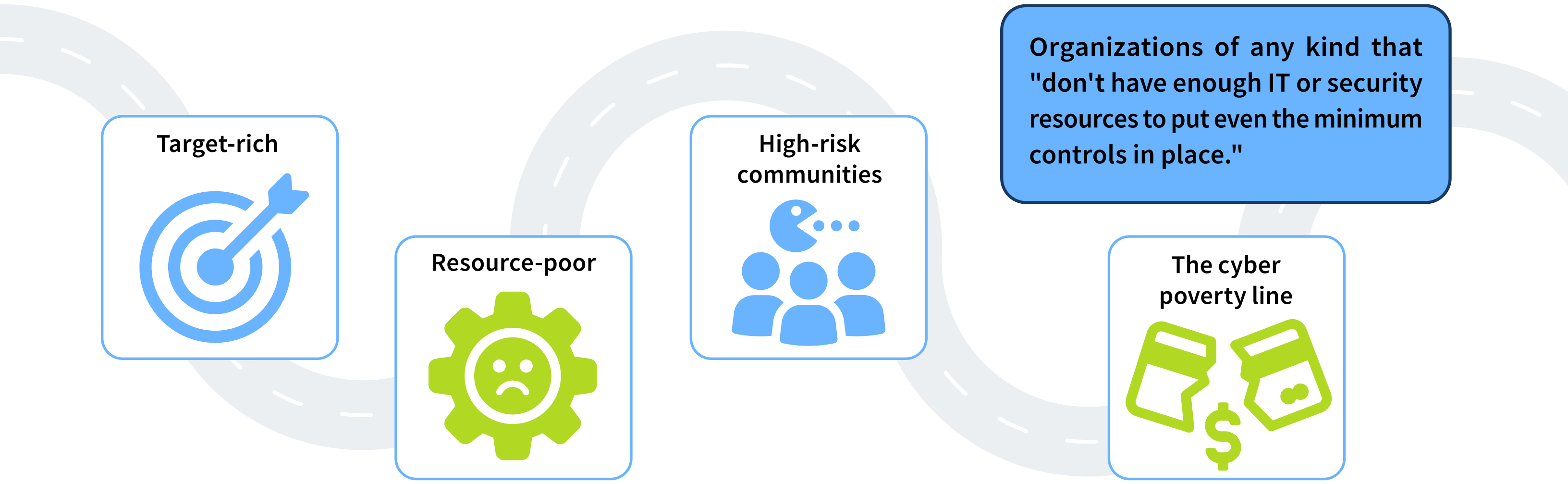
## Adding fuel to the fire, community organizations that face elevated cybersecurity threats also have fewer resources to protect themselves. Today, cybersecurity protections are available only for those organizations that can afford it, leading to a widening chasm between the "haves" and the "have nots."

There are many terms to describe organizations that cannot afford to protect themselves: "target-rich, resource-poor," "high-risk communities," and perhaps most commonly, those that fall below "the cyber poverty line," a term coined by Wendy Nather in 2011[15] to describe organizations of any kind that "don't have enough IT or security resources to put even the minimum controls in place." We refer to these organizations for the remainder of this report as "community organizations" to emphasize their contributions to the health and well-being of our society, and to cut across the public, private, and nonprofit sectors.

Disconnecting from the online space is not an option for community organizations; the internet now underpins our economy and nearly every service that people rely on for daily life. Without connected technology, public life comes to a halt entirely: schools close, ATMs stop functioning, and utilities do not get paid. Not only is disconnecting not an option, but connecting more services to the internet is becoming an expectation from customers and beneficiaries. As a result, the attack surface of community organizations increases each year, but their ability to manage the increased risks does not.

To make matters worse, with the rise of automation in cybercrime and ransomware-as-a-service (RaaS), many victims are attacked indiscriminately simply because they are using a digital system that has not been properly secured.

Despite the cyber field's tendency to focus on each sector individually, or to prioritize only those that qualify as "critical infrastructure," community organizations are inherently interconnected and interdependent, meaning that disruption in services in one can have cascading effects on others. For example, without clean water, hospitals cannot sanitize equipment or wash hands, delaying surgeries and forcing workarounds. Therefore, efforts focused solely on strengthening cybersecurity for hospitals may prove fruitless when an attack on a local water utility forces those same hospitals to postpone urgent surgeries. Community organizations are highly interdependent; just as hospitals need water, small businesses need childcare, and utilities need city governments, which in turn need nonprofits, and so on. The collective success of all community organizations is essential to safeguarding our public life.



Organizations of any kind that "don't have enough IT or security resources to put even the minimum controls in place."

## Community Organizations Cannot Afford Cybersecurity

The ongoing cost of cybersecurity far exceeds the budgets available to most small organizations. The median annual pay for an Information Security Analyst was $120,360 in 2023,[16] and the average annual pay for an IT Specialist at a nonprofit in 2024 was $65,000,[17] excluding healthcare and other benefits. The minimum cost of basic managed IT services starts at around $200 per user per month. When adding cybersecurity services, that number jumps to around $350 per user per month.[18]

**Figure 2**

### The Cost of Cybersecurity

**$65,000-$120,000**

**Average yearly pay for FTE**, excluding benefits

**$144,000**

Estimated **yearly cost of managed services** for IT and cybersecurity for a 50-person organization

**$4,200-$12,000**

Estimated **yearly cost of one cybersecurity tool**, such as a password manager, for a 50-person organization

For large corporations, these minimum costs are manageable. In 2024, the average corporate cybersecurity budget was less than 1% of total revenue (0.69%), equivalent to at least $690,000 for over 94% of IANS annual CISO Compensation and Budget Benchmark survey respondents.[19,20]

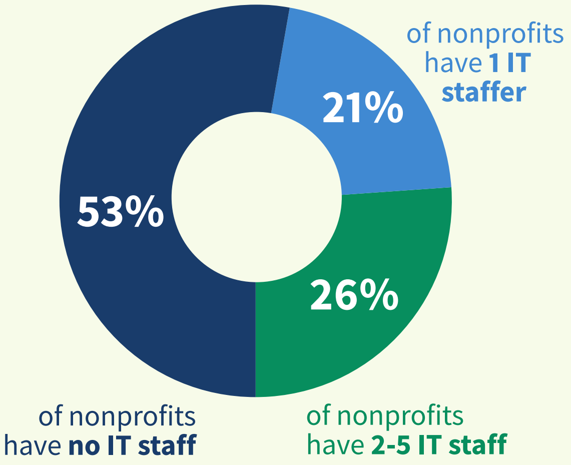
However, budgets at community organizations often lag far behind, especially at nonprofit and public entities that allocate the majority of their budgets toward mission-driven services. Based on the above figure, 1% of the average revenue of a single corporation ($690,000) is larger than the entire yearly budget for over 88% of nonprofits in the U.S. ($500,000).[21,22]

If nonprofits were to allocate the same percentage of their budgets to cybersecurity as corporations do, most would have just $6,900 or less per year for cybersecurity, putting full-time staff and contractors well out of reach. And indeed, 56% of NGOs do not have a budget allocated for cybersecurity.[23]

## Community Organizations Do Not Have In-House Expertise to Implement Cybersecurity

Compounding their funding challenges, community organizations often lack the in-house cyber expertise to protect themselves from cyberattacks. Many of these organizations have limited or no full-time employees dedicated to IT, let alone cybersecurity. For example, CLTC's CyberCAN project surveyed nonprofits in the Bay Area and found that 53% of respondents had no full-time IT staff, and those that did had an average of one IT staff member for every 96 employees.[24]

**Figure 3: Nonprofit Dedicated IT Staff**
[68 Responses]



Without the budget to hire one or more full-time IT or cybersecurity staff, community organizations are left with two options: to outsource IT and cyber expertise, or to hope existing staff will be able to cover the gaps. Both of these options are uphill battles, and without real people to provide assistance, community organizations face extreme difficulty navigating the cybersecurity product landscape and implementing safeguards.

The cyber field is plagued with information asymmetry that benefits companies and disadvantages community organizations. IT-Harvest, an industry analysis site, tracks over 10,000 cybersecurity products alone; with this saturation, it can be difficult for consumers to understand what to buy.[25] As stated in an April 2025 Lawfare op-ed,[26] Harry Coker, then-National Cyber Director, said, "There is no easy way for a customer — even, for example, a security-sophisticated chief information security officer — to understand if an IT product is secure."

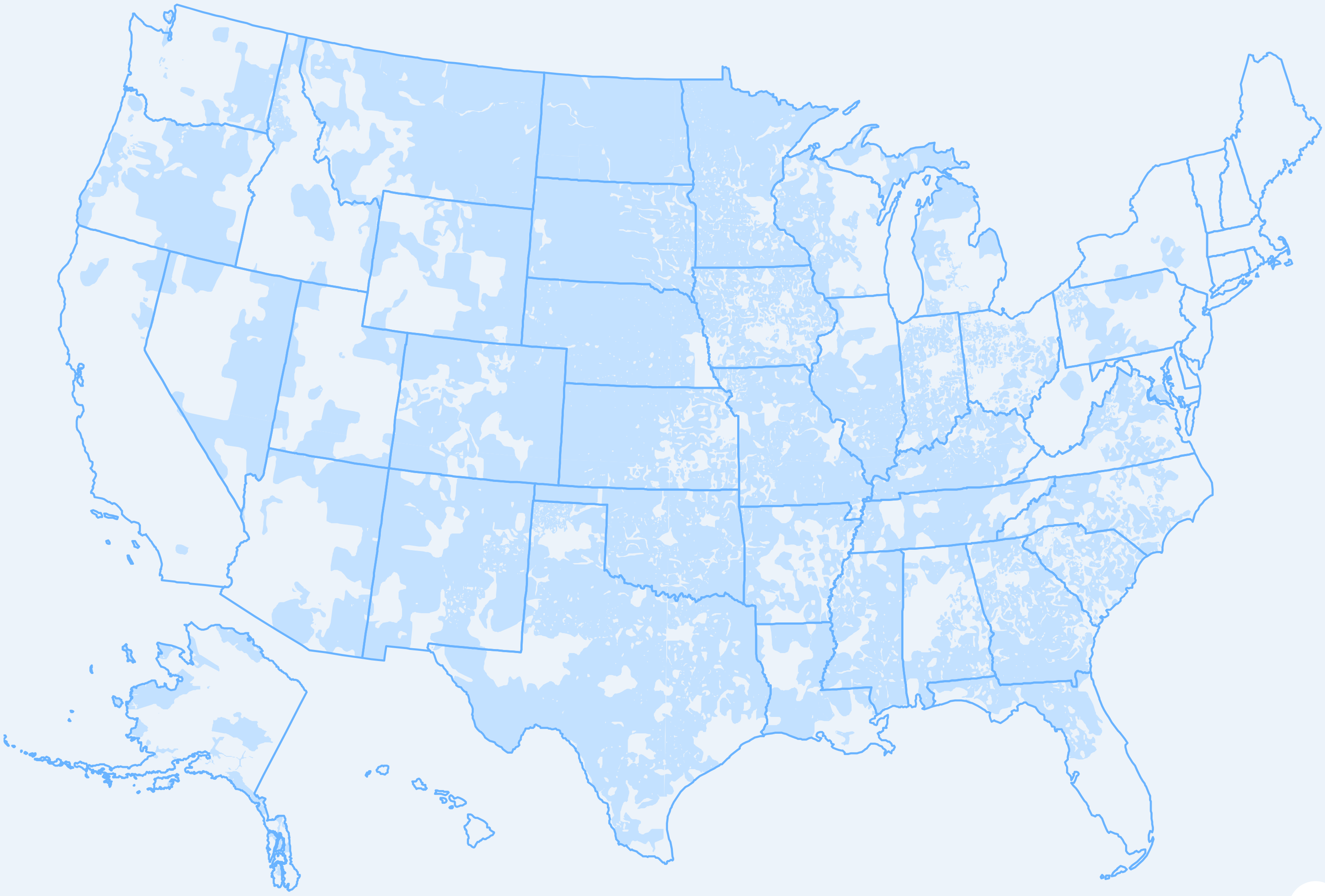
Even if an organization purchases "secure" products, the products may not be set up with the proper default configurations, and manual configurations are difficult for non-experts. Many products do not come with the most secure settings turned on (commonly referred to as "secure-by-default"), which means that organizations must know, understand, and implement the correct settings in order to securely configure their accounts. Even when software vendors provide guidance, such as the 17-page K-12 Guidebook released by Google in 2024,[27] unrealistic expectations persist about school administrators' time and capacity to successfully use such guidance. Though Google[28] and Microsoft[29] have since made progress in developing secure-by-default products — for example, by turning on multi-factor authentication (MFA) by default for certain accounts — products sold by most software vendors require a baseline of expertise to fully set up secure features.

# The Risks of Inaction

The connection between vulnerable populations and cyberattacks is severely understudied, but we are beginning to see evidence that cyberattacks ultimately hurt our nation's most vulnerable populations the most, especially people living in poverty or in rural areas.

**Figure 4** (Source: The National Rural Electric Cooperative Association (NRECA))

**Cooperatives power 56% of the American landscape**



First, residents of rural counties and people facing poverty are more likely to be served by small, at-risk organizations, which tend to be more vulnerable to cyberattacks. This can be seen in traditional utility services, such as power. As of 2017, almost three-quarters of utility customers in the U.S. were served by large, regulated, and investor-owned utilities. However, small, nonprofit electric cooperatives serve the vast majority of the United States in terms of geography, including 92% of counties that experience persistent poverty. According to a representative from the U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER), electric co-ops provide critical power to farms, towns, and small cities, but also "don't necessarily have access to the cybersecurity training, services, and technical assistance they need."[30]

Second, residents of rural counties and people facing poverty are least likely to be able to find services elsewhere when an organization that serves them is hit with a cyber attack. In 2020, a ransomware attack on the University of Vermont Medical Center forced their cancer center to turn away 75% of patients for nearly a month, leaving hundreds of patients without access to lifesaving chemotherapy medication.[31] Nurses shared that "many cancer patients who live in rural areas do not have the resources to drive four hours to Boston for treatment." Thus, the ultimate impact of the cyberattack fell more heavily on rural patients than on those in urban areas or those with greater access to resources.

In some cases, cyberattacks can lead to the complete loss of critical resources for those in rural areas who are already under strain. In 2021, St. Margaret's Health, a small hospital in rural Indiana, experienced a ransomware attack that sent it into a "financial spiral," and the hospital closed in 2023, reducing or removing care for the region's residents.[32] Over 151 rural hospitals have closed since 2010,[33] and many rural hospitals are at risk if a cyberattack proves to be one challenge too many.

Hospitals and utilities are not the only community organizations that can have their services interrupted by digital threats. Cyber attacks on food banks can result in reduced meals available for the hungry. Cyber attacks that close schools have a negative impact on children's learning, and especially strain working families and those who cannot afford childcare. Figure 5 provides additional examples of services that could be affected by digital threats, along with examples of the populations that would be affected by reduced services.

**Figure 5: Community Organizations and the Populations They Serve**

## Nonprofit Organizations (NGOs)

- **Critical services provided:** Housing assistance, legal aid, blood donation, food banks, job training, and other social services.
- **Populations served:** "Most nonprofits (55 percent) have programs that serve the general public, and 45 percent have programs that focus on people and families below the federal poverty level. Many organizations provide programs that focus on historically marginalized groups, including people who are Black or African American (29 percent), Latinx (27 percent), Indigenous, Native American, or Alaskan Native (17 percent), and LGBTQ (19 percent)."[34]

## Cities, Towns, and Other Local Governments

- **Critical services provided:** Fire, police, and emergency response, 911 call centers, food inspection, transportation, road maintenance, elder care, housing assistance, billing and permitting, real estate transactions, and other services.
- **Populations served:** All residents and visitors. The average poverty rate for rural (non-metropolitan) counties in 2022 was 15.5%, 3.4% higher than for metropolitan counties on average.[35]

## Water, Electricity, and Other Utilities

- **Services provided:** Clean water, sewage processing, trash disposal, light and power for homes, hospitals, and other fixtures of public life.
- **Populations served:** Nonprofit electric co-ops serve the vast majority of the U.S. geography, including 92% of persistent poverty counties.[36]

## K-12 Schools

- **Services provided:** Education, childcare, counseling services, free or reduced-price meals, workforce development, and special education services.
- **Populations served:** 83% of all U.S. pre-K through 12th grade students are served by public schools.[37] In the U.S., approximately 49.6 million students were enrolled in public elementary and secondary schools in the fall of 2022.[38]

## Small Rural Hospitals (100 beds or fewer)

- **Services provided:** Emergency medicine, labor and delivery services, surgery, diagnostic tests, laboratory tests, and mental health services.
- **Populations served:** "Rural hospitals in the United States serve an estimated 57 million people, representing about 20% of the total U.S. population."[39]

# Existing Solutions and Analysis

A variety of individuals have been working to address the gap in cybersecurity services for community organizations, and this context is crucial for understanding which solutions are most effective and what further action is needed. In this section, we provide an overview of the current products, tools, and services designed to close the cybersecurity gap, and then analyze what works well and identify the gaps that require immediate attention.

## Existing Solutions for Community Organizations

Current solutions for addressing the cybersecurity needs of community organizations approach the problem from varying angles. Most solutions can be classified as either a product, tool, or service, an important distinction when analyzing effectiveness for low-resource and low-staff organizations.

### Products and Tools

In the context of this report, “products” include, but are not limited to, licenses for cloud-based, IT, and/or cybersecurity software products. “Tools” refers to, but is not limited to, self-assessments, frameworks, toolkits, guides, and best practice guides. Tools are by far the most common and accessible category in the cybersecurity resource market. Both products and tools can help provide community organizations with the infrastructure to implement basic security practices and utilize monitoring systems.

Free products and tools abound, from self-assessment frameworks to best-practice guides, from network scanning to DDoS protection. Many products and tools are donated by industry, and many are excellent resources for protecting community organizations. This report does not attempt to discuss products and tools in detail or provide an exhaustive list; we are focused on the "services" part of the equation for community cybersecurity. To the extent that we discuss products and tools, it is to examine how direct services work in tandem with free products and tools, and how services can help community organizations take better advantage of the many excellent resources at their disposal.

Free tools on their own can also lead to the illusion of security: a community organization may deploy a firewall or an intrusion detection system that sends frequent alerts, creating a sense of taking action even though the organization is not equipped to respond to those alerts. If organizations use free tools that they cannot manage, and these tools prevent them from taking additional steps to reduce risk, it could leave them worse off than having no tools at all.

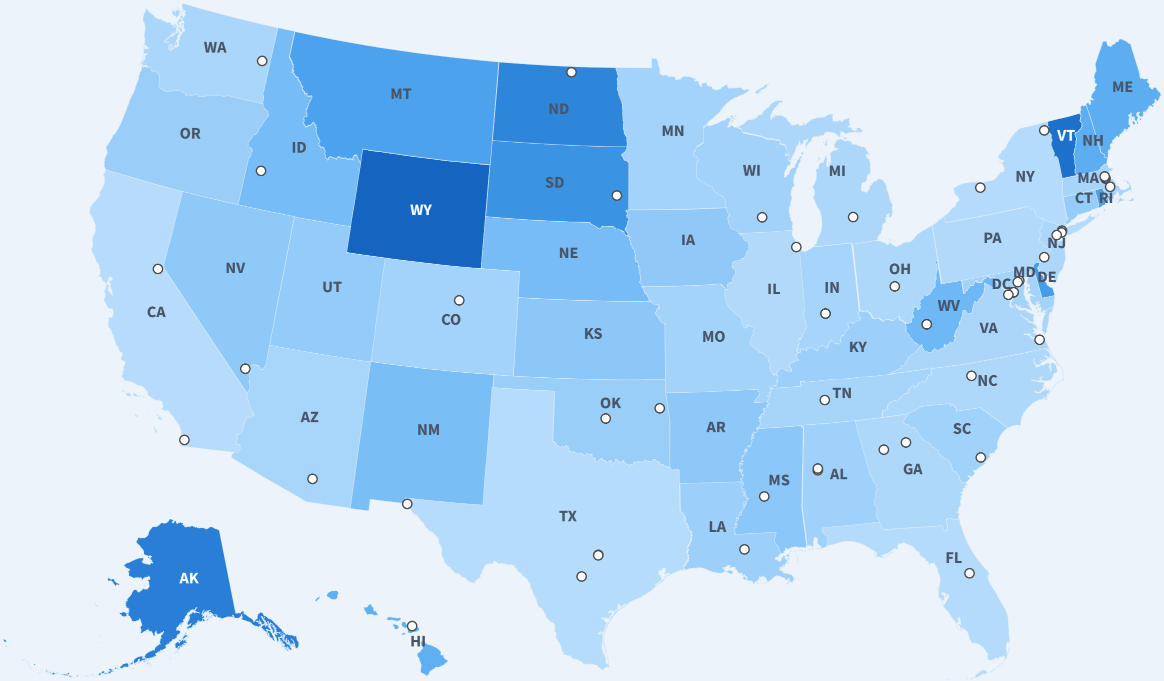
## Services

The term “services” refers to hands-on assistance, encompassing a range of activities from risk assessments to incident response and penetration testing. People are the key differentiator between tools and services: a tool can be downloaded, a guide can be read, but a service cannot be provided without another person interacting with an organization.

Over the last 15 years, new service-oriented organizations have been established to address the vulnerability of organizations operating below the cyber poverty line. Most of these organizations are composed of volunteers who offer pro bono services in their free time or for non-monetary incentives, such as school credit. Other service providers provide low-cost or significantly below-market cybersecurity services.

The Cyber Resilience Corps, by collecting data directly from cyber volunteering groups, estimates that as of May 2025, there are approximately 3,900 cyber volunteers in the U.S. spread across 50 volunteering groups. These volunteers currently help around 500 community organizations per year.

**Figure 6** (Source: The Cyber Resilience Corps Platform. www.cybervolunteers.us.)



**This map shows the distribution of volunteer networks across the United States, and the number of volunteers per million inhabitants, ranging from 0 (white) to 4.7k (dark blue). Darker blue indicates a higher concentration of local volunteer groups.**

## Several Types Of Cyber Volunteering Groups Offer Different Services In Various Locations To Diverse Beneficiaries

**State-led cyber corps** are groups of volunteer cybersecurity professionals who provide preventive and reactive cybersecurity services to beneficiaries. They can be organized by and operate under the authority of a government, nonprofit organization, for-profit entity, or a consortium of organizations. As of 2025, cyber corps programs are operational in Michigan,[40] Wisconsin,[41] Texas,[42] Maryland,[43] Ohio,[44,45] and Louisiana.[46]

**Nonprofit-led cyber volunteering groups** are cyber volunteering groups run by independent nonprofits, which often fundraise to support operations. They help match individual volunteers to organizations in need, generally for specific tasks such as router configuration or writing an incident response guide. Examples include the CyberPeace Builders,[47] CTI League,[48] and DEF CON Franklin.[49]

**Cybersecurity clinics** offer risk assessments and other services to community organizations, providing students with real-world cybersecurity experience. Modeled after legal[50] and medical school clinics, cybersecurity clinics are typically housed at colleges and universities and operate under the direction of clinical professors. Students from diverse backgrounds and degree paths train to provide free cybersecurity assistance to clients who would otherwise be unable to afford these services. Clinics serve as skills-based learning environments for students and as vital local resources for improving the cybersecurity resilience of communities.[51] Models like student-staffed security operations centers (SOCs) also help deliver detection and response services to local cities, counties, and school districts.

**Corporate volunteering.** Some for-profit cybersecurity and technology companies host programs that allow employees to volunteer a portion of their time to support organizations below the cyber poverty line. Some of these companies run their own volunteering programs, while others partner with nonprofit-based volunteering organizations, such as CyberPeace Builders or Apparo,[52] to match their employees with beneficiaries.[53] Additionally, several cyber insurance companies have established "centers of excellence" that provide cyber resources and education to community organizations.

**Government-subsidized services**. In 2022, the Cybersecurity and Infrastructure Security Agency (CISA) began offering no-cost cyber hygiene services to U.S.-based federal, state, local, tribal, and territorial governments, as well as public- and private-sector critical infrastructure organizations. These services include malware analysis, cyber resilience review, vulnerability scanning, cyber hygiene assessments, and automated threat indicator sharing.[54] Some state and local governments also offer similar services to qualifying community organizations.

**Information sharing organizations**. In specific sectors, Information Sharing and Analysis Centers (ISACs) are membership organizations that provide their members with services ranging from threat intelligence to incident response. Some ISACs most relevant to community organizations are the Multi-State Information Sharing and Analysis Center (MS-ISAC), Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), and NGO Information Sharing and Analysis Center (NGO-ISAC), which offer a variety of free services and resources. However, it should be noted that the smallest community organizations cannot often apply the threat intelligence supplied by their relevant ISAC.

**The National Guard**. At the state level, the National Guard can play a crucial role by assisting in response efforts during cyber incidents, helping community organizations bolster their cybersecurity resilience and recovery capabilities. Some states' National Guard units have dedicated cyber units that can be called upon to assist in incident response upon request by local entities, including critical infrastructure, cities, towns, and other organizations in need.

**Other innovative service models** have emerged that combine aspects of pro bono or below-market services with volunteering. For example, Sightline Security is a nonprofit that offers heavily discounted risk assessments to other nonprofits in need. Apparo, another nonprofit, works with corporate partners to pair nonprofit organizations below the cyber poverty line with volunteers and discounted tools. Indiana Cybertrack, a partnership between the Indiana Office of Technology and local universities, offers free risk assessments to local governments while training students, thereby providing the state with valuable insights into the cyber maturity of city governments.

# What Works? Lessons Learned

Cyber Resilience Corps working group members highlighted several key themes that program leaders have learned from years of practice.

## Services Are Needed to Complement Products and Tools

Free tools and products can help bolster an organization's security posture, but they only take an organization partway to solving its problems. Hands-on, human support is often necessary for community organizations to leverage products and tools fully.

Services, such as consulting or risk assessments, meet community organizations where they are, and can be customized to each organization's infrastructure. Services help community organizations extend their limited staff by outsourcing specific cybersecurity expertise. Services that enable a community organization's staff to ask questions are more accessible to people of all knowledge levels in cybersecurity and are therefore more effective.

## Relationships Between Service Providers Support Systemic Resilience

CRC members emphasized that relationships between volunteer program leaders and other local community leaders provide the critical connective tissue necessary for providing continued support to beneficiary organizations. State cyber corps programs that collaborated with various stakeholders, including cyber insurers and managed service providers (MSPs), were able to expand their impact. For example, the Wisconsin Cyber Response Team has received valuable referrals from two cyber insurers, which helped connect community organizations to the response team's services.[55] In another example, the University of North Carolina at Charlotte's cybersecurity clinic partners with local nonprofit Apparo to connect beneficiary organizations with further cybersecurity support.

Dedicated bridge-building between state cyber corps programs, university cyber clinics, community organizations, and cyber insurers helps break down barriers for organizations that choose to work with state cyber corps to access cyber insurer services. However, this kind of bridge-building remains the exception rather than the norm.

## Community Organizations Are Best Served by Those Who Understand Their Unique Challenges and Needs

Continuous security support is critical to improving community organizations' cyber resilience, which is why their relationships with service providers play a key role in their overall defenses. Based on our conversations with CRC members, community organizations prefer providers with experience working with similar types of organizations, which often have different sets of concerns, priorities, and capabilities than do larger businesses.[56]

Service providers with prior experience working directly with smaller organizations have the advantage of understanding how to address their unique circumstances. These service providers may be more accustomed to understanding and advising small community organizations on the most immediate and essential security steps, and can contextualize their services across variations in geography, culture, language, nonprofit status, and organization size. Helping these often resource-strapped organizations discern what services they do not need can be invaluable in assisting them to maximize their resource allocation toward actions that directly align with their missions.

## Information Sharing Enhances Overall Security Posture

Increased information sharing is one lever that has helped strengthen the digital defenses of community organizations. For community organizations, especially those with operational technology (OT), which refers to hardware and software that directly interacts with and controls physical processes, devices, and infrastructure within an organization, ISACs (including MS-ISAC, EI-ISAC, E-ISAC, REN-ISAC, NGO-ISAC, and many more) can provide education, information sharing, networking, and workshops on emerging technologies and threats, which helps build resilience across organizations.[57]

In a significant leap forward for the security of governmental organizations, in 2019, the Cybersecurity Infrastructure and Security Agency (CISA) launched the ambitious State, Local, Tribal, and Territorial Cyber Information Sharing Program. With help from the Johns Hopkins University Applied Physics Laboratory (JHU/APL), this program conducted a pilot project to enhance the cybersecurity defenses of state, local, tribal, and territorial (SLTT) governments across the United States. The Multi-State Information Sharing and Analysis Center (MS-ISAC), composed of thousands of members nationally, played a key role in the program, providing many services to constituent state and local governments, including sharing intelligence briefings on emerging cybersecurity threats, notices on the latest security patches, incident response support, and penetration testing.[58]

While data about the full impact of these programs is not available to the public due to national security concerns, the National Association of State CIOs has cited these information-sharing programs as being "tremendously beneficial" to state and local governments.[59]

# What Gaps Remain? Where Solutions Fall Short

Cyber Resilience Corps members identified several gaps that existing programs are unable to cover, as well as common problems that service providers face nationwide.

## Volunteering Services Are Not Equally Accessible

While existing volunteer-based programs are making headway in providing cybersecurity assistance to community organizations, free services are not yet widespread enough to help everyone. As of May 2025, we estimate that there are only 3,900 volunteers distributed among 50 cyber volunteering organizations across the U.S. At least 22 states do not have any regional or local volunteering groups, including university clinics or state cyber corps. Locally based volunteering groups are beneficial because they can deploy “boots on the ground” to help community organizations in rural locations and other regions where the tech industry presence is limited. However, locally based volunteering groups may be limited in the organizations they can serve by their founding legislation, funding model, or other logistical restraints.

Ultimately, the limited size and regional coverage of cyber volunteering groups mean that some community organizations in need may not be able to receive free cyber services. Where demand for services is exceedingly high, national volunteering organizations may be forced to prioritize services for organizations that are the most vulnerable or actively in crisis. Smaller community organizations that are not in crisis or whose missions are perceived as less critical may be deprioritized and fall through the cracks.

## Organizations Do Not Know Where to Go

While free and reduced-cost cybersecurity services can be immensely valuable, our research suggests that most community organizations are unaware of these services. Currently, there is no centralized way to identify what services are available or which organizations qualify, leaving the research burden to organizations whose time is already limited. CISA took a first step in cataloging volunteer cyber resources through its Cyber Volunteer Resource Center,[60] but the list is not exhaustive, and the site is not regularly updated. States should take a leading role in directing their community organizations toward regional and local cyber volunteering organizations.

## Legal & Liability Challenges Create Barriers to Volunteering Services

Legal and liability questions have been a significant speed bump for volunteering organizations' ability to serve community organizations in need of services. Agreements between the individual volunteer, the volunteer group, and the community organization are necessary to protect all parties involved. In some cases, such as when companies allow their employees to use portions of their working hours for cyber volunteering, an additional agreement may be necessary between the private organization and the volunteering group. Creating these agreements can be complicated, often requiring expert legal counsel; however, some basic templates do exist to help guide organizations.[61] There can be significant time and financial costs associated with getting these agreements in place. These issues can hinder the ability of volunteering organizations to provide services to community organizations in need, as well as to scale the number of volunteers ready to help.

The burden of ensuring adequate liability protection is particularly acute for volunteer groups that provide incident response support. Getting proper liability protection in place can increase a volunteer group's time to respond to an active incident and can limit the types of volunteering organizations that can assist. Incident response is also a relatively specialized skill, with a limited number of individuals possessing the requisite level of experience to be effective. Any obstacles to enlisting and deploying the help of these skilled individuals in a volunteering capacity can have an outsized negative impact on community organizations in need.

## Government Funding for Services Can Be Volatile

Federal funding sources have historically provided much-needed financial support aimed at community cybersecurity. When this landscape changes, it leaves gaps that are difficult for other actors to fill. For example, as of early March 2025, roughly half of MS-ISAC's annual budget, totaling $10 million, is set not to be renewed after the conclusion of the fiscal year.[62] During a "town hall" meeting of the MS-ISAC membership following the announcement of the cuts, member representatives responded to a poll in which 97% said they considered MS-ISAC to be of "high value." Additionally, 83% of members said their organizations would not easily be able to find alternatives if the MS-ISAC's services were to disappear.[63]

Programs like the State and Local Cybersecurity Grant Program (SLCGP) and the Tribal Cybersecurity Grant Program (TCGP) have also provided much-needed financial and functional support to local governments, particularly to those in under-resourced, rural areas, allowing more communities to strengthen their cyber hygiene. While data on the direct impact of these programs is still largely unavailable, due to how recently the program began administering funds and how different states have chosen to implement the grants, anecdotal success stories underscore the program's effectiveness in driving tangible improvements in the cybersecurity posture of participating entities.

Without reauthorization from Congress, however, both the SLCGP and TCGP are set to expire in 2025. This volatility in government funding can have significant and disastrous impacts on community organizations. Budget cuts to key, wide-reaching federal cybersecurity programs can force budget-strapped organizations to delay crucial security updates and potentially reduce spending on advanced security measures, making them vulnerable to cybercriminals and adversaries.

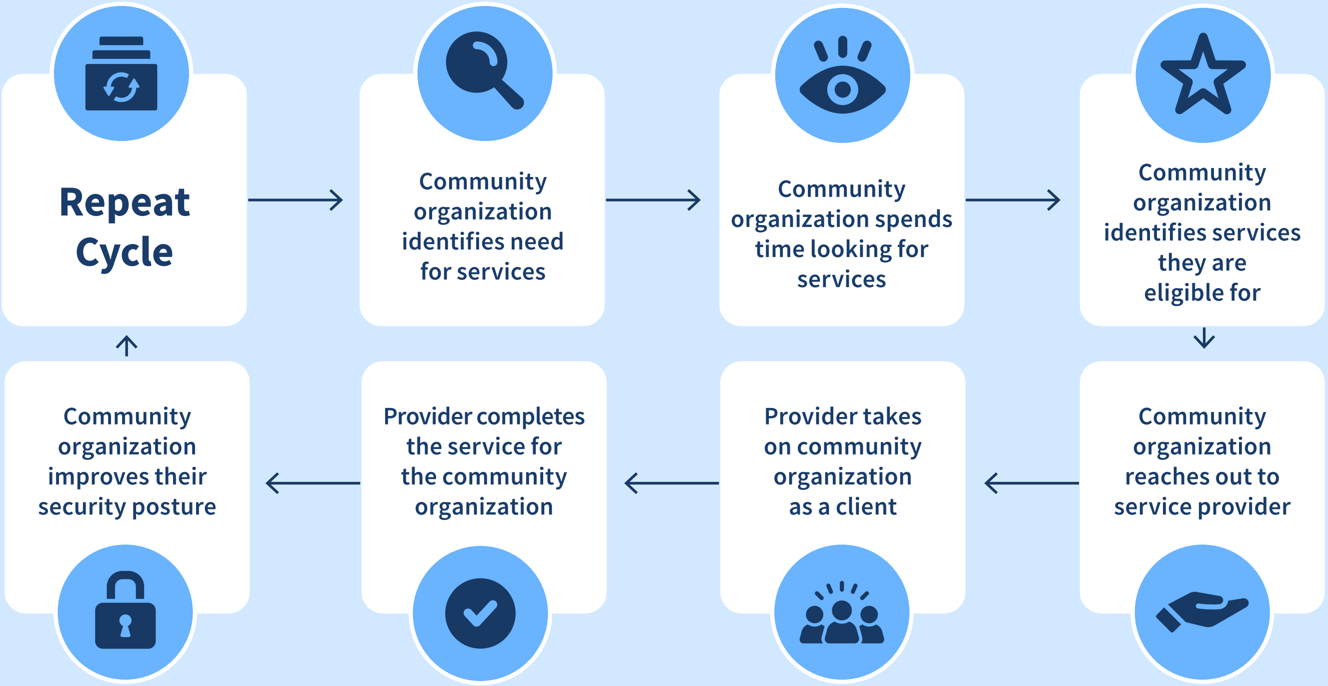
## The One-Time Engagement Model Creates Challenges

While not all volunteering engagements are exclusively available on a one-time basis, most providers of free services are not able to provide continual support for the organizations they serve. The length and depth of engagements can vary significantly between service providers; however, the services typically conclude at the end of the engagement.

Because of this, there are significant drawbacks to volunteering as a primary solution. In most existing pathways for community organizations seeking cybersecurity help, services are only rendered after the beneficiary identifies the available services, determines their needs, and confirms their eligibility.

In the current system, community organizations without dedicated IT or security staff often treat cybersecurity as a one-time problem to be solved. They make tangible and measurable improvements to their security posture while services, such as those provided by volunteer organizations, are rendered. Yet they often lack the financial resources, human capital, and guidance to respond to evolving threats and technologies after the volunteer engagement concludes.

Particularly when the service rendered is an assessment, organizations can be left without the capacity to implement the recommendations they have received. Many cybersecurity best practices require a certain level of IT maturity. Even if organizations can obtain cybersecurity support, they may not have the resources to continually improve their IT support and infrastructure as required to maintain cybersecurity best practices on an ongoing basis.


Repeat Cycle
Community organization identifies need for services
Community organization spends time looking for services
Community organization identifies services they are eligible for
Community organization reaches out to service provider
Provider takes on community organization as a client
Provider completes the service for the community organization
Community organization improves their security posture

## Programs Face Difficulty Collecting Standardized Metrics on Impact

Collecting standardized metrics would help prove the impact of cyber volunteering services and create opportunities to learn more about the organizations they serve. While some standardized evaluations exist, such as Indiana's CyberTrack,[64] in most cases measurement practices vary widely across different programs, making it difficult to assess how cyber volunteer services collectively shape improved cybersecurity postures and practices. Without consistent metrics across programs, leaders of volunteer services may be able to understand which organizations have benefited and what services were provided, but not be able to assess their long-term impact.

It is also challenging for volunteer programs to evaluate the long-term impact of their interventions due to the one-time nature of many cyber volunteering engagements. For example, it can be difficult to determine whether a one-time risk assessment can improve outcomes for an organization a year after the intervention has been implemented. Without a formal feedback mechanism and continual re-engagement of past clients, it is very difficult to determine the answers to such longitudinal questions. Particularly in cases where a program provides incident response services and does not re-engage, the client organization may not fully grasp the necessity of ongoing, continuous cyber hygiene education and vigilance.

Additionally, there is often significant turnover at both beneficiary and volunteer program organizations, which can make tracking impact and effectiveness even more challenging as institutional knowledge is lost amidst staff turnover.

## No Continuum of Support for Community Organizations

Cyber risk is dynamic; the frequency and complexity of threats to community organizations continue to accelerate. Having a system for continued support is imperative. However, at this point, the overall cyber volunteering ecosystem lacks a standardized or centralized process for handoffs between service organizations. As cyber volunteer services are typically one-time engagements, community organizations often do not have ongoing support after an engagement ends.

While a small handful of cyber volunteering organizations refer clients to ongoing service providers, the practice is not widespread. In interviews, volunteer service providers expressed concern about the risks of referring community organizations to ongoing service providers, citing a few key reasons:

1. The majority of volunteer-based service providers operate as nonprofit groups, and as such, they are able to build trust with their beneficiaries. Both the service provider and the community organization are guided by their primary missions, rather than profit. Some volunteers expressed hesitancy about referring a beneficiary to a for-profit company for ongoing services out of fear that the community organizations would be taken advantage of.

2. Volunteer service providers may feel unprepared to refer their clients to ongoing service providers. There are currently estimated to be hundreds of managed service providers (MSPs) in the United States, many of them small and regionally focused.[65] The difference in quality between MSPs can be substantial, but difficult to discern without direct experience. As a result, volunteer service providers may choose not to make a referral to an ongoing service provider because they do not feel prepared to offer their endorsement.

A consistent and reliable off-ramp that provides continued support and services for community organizations following an engagement with a service provider, such as a state cyber corps or cyber clinic, would help build widespread, ongoing resilience.

# The Roadmap to Community Cybersecurity

A coordinated strategy is necessary to defend community organizations, including local governments, schools, and nonprofits, both in the short term and in the long term, to create a society where all organizations can thrive, regardless of their resources or cybersecurity expertise.

This report has outlined the cyber risks that community organizations face, highlighting where existing solutions are successful and where they fall short.

**In this section, we outline a path forward, a strategic approach that cybersecurity and policy leaders can take together to create a world where our public life is secure.**

### A Cyber Co-Responsibility Model

We begin by charting a model in which community organizations maintain a reasonable level of responsibility for their cybersecurity, but without the current burdens of the overly complex cybersecurity ecosystem.

### The On-Ramp

We then propose an "on-ramp," a set of short-term recommendations that, if adopted, will make a measurable difference in our collective ability to defend community organizations from cyber attacks, leaning heavily on cyber volunteers.

### Our Destination

We describe a long-term vision in which community organizations are collectively more secure, with an overview of broad interventions necessary to move the United States in that direction.

### State Guidebook: Creating a Regional Cyber Support Ecosystem

We conclude with a guidebook for how leaders at the state level can strengthen local ecosystems of cyber support and improve the level of resources available to community organizations.

# 1 A Cyber Co-Responsibility Model

## We cannot envision a better cybersecurity future without reassessing and redistributing the responsibilities of individual organizations.

The question of community organizations' responsibility to defend themselves against rising external threats has been ongoing and omnipresent in cybersecurity discussions for years. Most notably, in 2023, the White House Office of the National Cyber Director (ONCD) under the Biden Administration released the National Cyber Strategy, which prominently highlighted the unfair burden organizations are forced to carry to protect themselves. The strategy called for "shifting the burden for cybersecurity away from individuals, small businesses, local governments, and infrastructure operators, and onto the organizations that are most capable and best-positioned to reduce risks for all of us."[66]

But what exactly does "the burden for cybersecurity" encompass, and what is a reasonable expectation for how much of this burden organizations should carry? This question drove much of the Cyber Resilience Corps' discussion and led to the following framework:

### Community organizations **SHOULD** be responsible for:

- Understanding cybersecurity risk
- Seeking and advocating for solutions to those risks

### Community organizations **SHOULD NOT** be responsible for:

- Being cybersecurity experts
- Hiring in-house cybersecurity experts

## Community Organizations Should Keep One Hand on the Wheel

In group discussions, the CRC was firmly aligned around the idea that some responsibility must always reside within community organizations themselves. Whether it be a hospital, nonprofit, school, or city government, community organizations are accustomed to understanding risks specific to their work. For example, to remove entirely a school's responsibility to wrestle with cybersecurity would be to infringe on its autonomy to make informed decisions about educating students and protecting their data. It would also create a moral hazard, where cybersecurity is continually "someone else's problem," leading organizations to underinvest in cybersecurity.

We propose that community organizations should be primarily responsible for understanding cybersecurity risks relevant to their business and for seeking and advocating for solutions to those risks.

## Community Organizations Should Not Be Mechanics

The beauty of living in a technologically advanced society is that tools are widely available, and one need not understand them to make use of them. Cars are an excellent example of this; few could tell you how an engine works, let alone repair one, but nearly everyone can learn to drive.

Currently, when it comes to cybersecurity, community organizations are expected to build the car they're driving — to know how the car works, what different parts they need, how those parts work together, and how to perform routine maintenance in a world where a new model comes out every month. In short, they're expected to be (or hire) cybersecurity experts simply to maintain their day-to-day existence.

This current distribution of responsibility is not only unfair, it is ineffective. As detailed in Section 1, community organizations are often unable to defend themselves against cyberattacks effectively, and as threat actors continue to improve and cybersecurity becomes increasingly complex, the challenge will only worsen.

We propose that small community organizations should not be responsible for being cyber experts to do business or provide a public service. They should not need to understand the intricacies of different attack vectors or how to configure their software for optimal security in order to provide their services and fulfill their missions.

## Not Everyone Needs a Full-Time Mechanic

One way to shoulder the unequal burden of cybersecurity is to hire a full-time IT and/or cybersecurity staff member, but this is too expensive for many community organizations; as part of the whitepaper "CyberCAN: Cybersecurity for Cities and Nonprofits," CLTC surveyed 68 nonprofits in the San Francisco Bay Area and found that 53% had no full-time IT or cyber staff at all, and nearly all the rest had 1-2 full-time staff.[67]

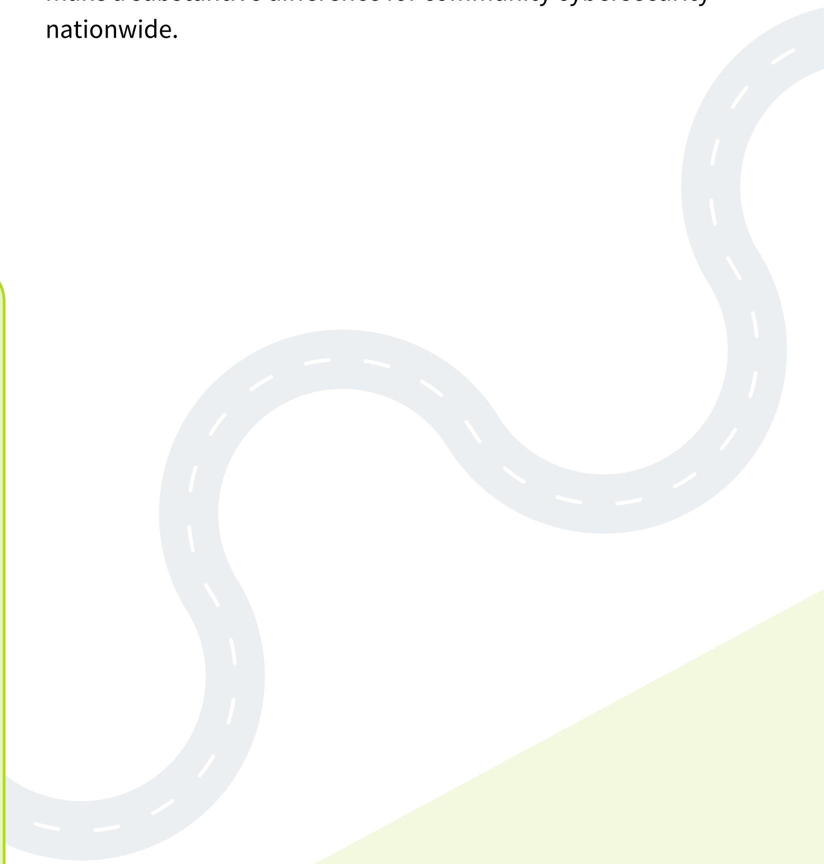
Some companies may always need in-house expertise. For example, large enterprise businesses, especially those dealing with sensitive information (e.g., banks) or those with substantial sums at stake in product availability (e.g., communications or technology), may spend millions of dollars per year on cybersecurity and employ hundreds of cybersecurity employees.

However, the expectation of employing internal, full-time cybersecurity talent cannot be applied uniformly, especially to organizations with limited budgets that cannot afford to hire even one cybersecurity expert on a permanent basis. Our "north star" is that every nonprofit or small business should be able to succeed without a cybersecurity expert on payroll.

## Themes from Cyber Co-Responsibility

By understanding exactly what responsibilities should shift away from individual organizations, the CRC was able to propose targeted solutions to make the most impact. Out of all the recommendations that would make a difference for community organizations, we prioritized solutions that would incentivize organizations to invest in understanding their cybersecurity risks and seeking solutions to mitigate them.

These are by no means the only actions that can be taken, but our panel of experts feels they are the most likely to make a substantive difference for community cybersecurity nationwide.



As detailed further in the following section, our recommendation for the near term (i.e., the next two years) is to scale free and low-cost cybersecurity services, especially cyber volunteering programs, for the benefit of small community organizations. To sustain progress over time, we also recommend a five-year effort to simplify cybersecurity for non-experts and create pathways for long-term support.

# 2 The On-Ramp

## Address Immediate Ecosystem Needs

Cybersecurity support for community organizations cannot wait for long-term change. To address immediate gaps in services, we propose three broad interventions, containing nine specific recommendations, that rely on maturing and expanding cyber volunteering programs to rapidly assist our local schools, cities, nonprofits, and utilities.

**These recommendations fit into three broad categories:**

**Mature Cyber Volunteering Programs**

**Expand Cyber Volunteering Programs**

**Enhance Continuity of Service After Volunteering**

We are also ready to solve some of these immediate ecosystem needs today. As part of the Cyber Resilience Corps initiative, the CyberPeace Institute has launched a first-of-its-kind public website (www.cybervolunteers.us) to track cyber incidents and response efforts, including volunteer efforts, in real-time, highlighting the impact of cyber volunteers. The site includes a platform to help volunteer groups work together more easily, share resources, and coordinate responses; it also helps community organizations identify which volunteer service providers are available to them based on their location, type of organization, and services needed.

The cybervolunteers.us site aims to support a more coordinated and centralized resource to connect potential volunteers and beneficiary organizations, and to understand the impact of cyber volunteering groups broadly. Learn more at www.cybervolunteers.us.

## Mature Cyber Volunteering Programs

### #1 Expand collection of metrics on volunteer groups' impact.

Cyber volunteer programs should develop systems for tracking the effectiveness of their services over time and publish transparency reports regularly. While total standardization of measurement across all groups may be unfeasible, collecting a few key metrics on an annual basis — including the number of volunteers, the number of client organizations served, and the supply-to-demand ratio for their services — would be a valuable first step.

Cyber volunteering organizations can look to metric collection systems[68] developed by other cyber volunteering organizations as examples, including Indiana's CyberTrack, which is notable for measuring the effectiveness of their program through assessing how many, and how well, previously recommended actions were implemented by the organizations they have served.[69]

### #2 Clarify liability protections for cyber volunteering.

To reduce confusion about liability, the Cyber Resilience Corps should develop a centralized resource outlining state laws and statutes related to volunteers, identify best practices for other states to replicate, and increase volunteer groups' access to pro bono legal advice. The Cyber Resilience Corps and cyber volunteering programs should also promote training and awareness around liability issues and develop a short module on risk, statutory protections, and agreement mechanics.

Volunteer groups should adapt or adjust existing template agreements to include a statement of work, clear non-employment language, statutory access consent,[70] mutual confidentiality, and release and indemnity clauses.[71] Cyber legal clinics or law firms can also provide pro bono review of liability provisions for nonprofits or qualifying clients. A longer-term goal would be to maintain a panel of volunteer attorneys or firms who can advise cyber volunteer programs on legal issues.

### #3 Improve volunteer and client matching.

Cyber volunteering programs should develop resources to make it easier for both volunteers and clients to understand what volunteering groups are available, as well as where they operate and what services they provide.

Online platforms should be developed that seamlessly direct relevant expert volunteers to existing volunteer groups. These platforms should also streamline community organizations' ability to identify which volunteer organizations' services best fit, based on their needs and location.

Streamlining the processes for prospective volunteers and clients should bolster the capacities of existing cyber volunteering groups, increasing both the number of volunteers and the number of community organizations they can serve. The Cyber Resilience Corps' site, cybervolunteers.us, aims to take the first steps at addressing this recommendation.

## Expand Cyber Volunteering Across the United States

### #4 Prioritize the most threatened organizations.

Existing cyber volunteering programs should prioritize assistance for organizations that provide critical services and whose disruption is most likely to have a cascading effect. Providing services to critical infrastructure community organizations, such as water or electric utilities, that supply vital resources to other community organizations, like hospitals, will create upstream resilience of key services for communities.

### #5 Invest in interconnectivity among volunteer programs.

Cyber volunteering programs should enhance sharing of threat intelligence information and establish mechanisms to regularly share best practices, which will help nascent organizations scale and build nationwide resilience.

The Cyber Resilience Corps should invest in convening workshops and other opportunities to share creative solutions to protect vulnerable public infrastructure against cybersecurity threats.

### #6 Invest in cyber volunteering.

Philanthropic organizations, including private philanthropists, corporate donors, and foundations, should invest in expanding cyber volunteering programs, especially in states that currently lack programs and in high-population states that do not have enough volunteers to meet demand. Philanthropic support could come through direct funding or through the establishment of a collaborative fund for cyber volunteering.

The U.S. government should expand federal funding for state and local communities to improve their cyber resilience. In particular, the State and Local Cybersecurity Grant Program (SLCGP) and the Tribal Cybersecurity Grant Program (TCGP) should be renewed and extended to include direct services, including volunteering services. Additionally, Congress should renew the Cybersecurity Information Sharing Act of 2015[72] to support state cyber corps' ability to assess threats and recognize potential indicators of compromise (IOCs) at community organizations.

## Enhance Continuity of Service After Volunteering

### #7 Centralize key template resources.

The Cyber Resilience Corps should develop a comprehensive bundle of resources to help community organizations continue to invest in cybersecurity following their engagement with a volunteer group.

These resources can include template policies, such as an incident response plan, password policy, and a business continuity/disaster recovery plan tailored specifically for community organizations. These documents should build on industry best practices and the hands-on experience volunteer groups have gained by working with community organizations.

### #8 Bolster hand-off procedures after engagements.

The Cyber Resilience Corps should ensure that volunteer groups have trusted, standardized pathways to support beneficiaries' cyber maturity journey once the volunteer engagement concludes.

This should include handoffs to other complementary volunteering services; for example, a cyber clinic working with a city government can connect them to the state cyber corps as a resource to contact in case of a cyber incident. It should also include handoffs to other free and low-cost tools; for example, a corporate volunteer working with a nonprofit can point them toward TechSoup, a nonprofit that offers discounted IT and cybersecurity products for select community organizations.

### #9 Help organizations find full-time support.

The Cyber Resilience Corps should produce guidance on contracting with service providers to empower community organizations to advocate for themselves during the MSP/MSSP procurement process.

It is crucial for community organizations to transition from one-time volunteering engagements to receiving long-term support from a highly rated MSP or MSSP that works well with their specific needs. The CRC's guidance can help these organizations better understand the procurement process, effectively evaluate potential vendors, and identify key elements to look for in a contract.

# 3 Our Destination

## Create Long-Term Support and Ease the Burden on Individual Organizations

## Long-Term Interventions

### Companies must simplify cybersecurity for non-experts.

The staffing and knowledge burdens on community organizations are too high; we must alleviate these burdens by making cybersecurity accessible to non-experts.

The federal government plays a key role in simplifying cybersecurity. CISA should continue its leadership on the Secure-by-Design initiative (https://www.cisa.gov/securebydesign) and track and publish the progress of organizations that have made secure-by-design and secure-by-default commitments. (Secure-by-design[73] products are secure to use out of the box with minimal to no configuration changes, and they include security features at no additional cost to the consumer.)

In line with the National Cybersecurity Strategy, the U.S. Government should continue to shape and enforce software liability laws and regulations to hold companies accountable for releasing vulnerable software.

The private sector can also play an outsized role in making cybersecurity more accessible by voluntarily implementing secure-by-design and secure-by-default in software products and using those as competitive advantages. Companies can also continue to innovate in developing usable technology and offering affordable IT services that emphasize automation, allowing staff without cyber expertise to use other products securely.

Venture capital investors should continue to invest in developing low-cost cybersecurity products that automate essential cybersecurity actions and can be managed and operated by non-experts.

## Create Long-Term Support and Ease the Burden on Individual Organizations

### Long-Term Interventions

#### States should create shared services for community organizations.

Community organizations do not have enough hands-on support and often lack resources for professional services. Many small organizations also report difficulty contracting with large enterprises due to their size. States can vastly improve cybersecurity support at the local level by creating “shared services,” pooling critical resources for small organizations like cities, nonprofits, and utilities. (The shared services model is not new: for example, the UN International Computing Center provides at-cost, shared services for all UN affiliates.)

Shared services at the state level would allow community organizations to gain access to critical services at a discount or at cost while avoiding painstaking procurement and legal reviews. It would also allow states to better protect large numbers of local organizations, and enable companies to fill a market gap and create customers out of previously unserved organizations. Pooling dozens or hundreds of organizations into a single shared services contract could create incentives for private companies to serve community organizations.

Shared services should start not with products, but with critical services, including managed IT and cybersecurity services (e.g., risk assessment and implementation, security operations center (SOC) capabilities, and incident response), as well as protections that may drive investment in cyber hygiene, like cyber insurance. Shared services could be pooled for specific sectors in which domain expertise and trusted relationships in the community are essential; for example, a shared SOC could be established for the water sector, or a set of risk assessments could be developed for city governments.

It is also essential that the federal government continue to fund existing shared services for public infrastructure by MS-ISAC and CISA, including free monitoring, penetration testing, threat intelligence, and other federally subsidized services.

## Create Long-Term Support and Ease the Burden on Individual Organizations

## Long-Term Interventions

### We must embed cyber knowledge in our communities.

Free or inexpensive cyber education resources are widely available, but many organizations have not taken advantage of these opportunities. We must improve cyber education to help organizations better understand their internal risks and advocate for themselves when working with vendors.

As part of this effort, we must invest in developing trusted messengers from the cyber community and beyond to help organizations understand their role in cybersecurity, including how they can understand and evaluate risk, and make smart business decisions to abate that risk. Such messengers could be community leaders from a variety of contexts, such as loan officers at credit unions, representatives from small business administrations, or volunteers from local United Way chapters.

We must also continue to embed basic cybersecurity concepts in the American education system, as proposed in the National Workforce and Education Strategy. It is crucial for everyone to have personal cybersecurity awareness skills; learning these skills at a young age creates local workforces that are better equipped to deploy cybersecurity best practices and protect themselves and their loved ones from harm. After all, community security is national security.

# 4 State Guidebook: Creating a Regional Cyber Support Ecosystem

State governments are being asked to take on more responsibility for cybersecurity than ever before. A March 2025 Executive Order titled "Achieving Efficiency Through State and Local Preparedness" pushes states to "play a more active and significant role in national resilience and preparedness."[74]

However, state budgets are threatened as the federal funding landscape shifts, while state responsibilities are dramatically increasing as federal agencies —including CISA, the Department of Education, the Department of Energy, the Department of Justice, and many other sector-risk management agencies — are losing critical staff.

State government agencies cannot undertake this work alone, and states have the opportunity to establish regional cyber support ecosystems that can sustainably protect their residents in the long term. Mature regional ecosystems can comprise cyber defense programs from state governments, higher education institutions, and nonprofits that provide critical support to under-resourced organizations, including nonprofits, schools, utilities, hospitals, and cities, when they need it most, at little to no cost to the beneficiaries.

In this Guidebook, we centralize information on the three most popular regional cyber defense programs: cybersecurity clinics, state civilian cyber corps programs, and nonprofit volunteering groups. We then provide key interventions that states can take to expand these programs locally and improve the resilience of their communities while investing in home-grown talent.

# Regional Cyber Defense Programs

Protecting under-resourced organizations across a state is no small feat; many organizations have vastly different budgets, technologies, and missions. However, several proven models have been developed to help small organizations better protect themselves from cyberattacks, and states can provide broad support to cities and counties by funding programs that offer free or low-cost cybersecurity services.

**Cyber Clinics**

**State Civilian Cyber Corps**

**Nonprofit Volunteering**

# Cybersecurity Clinics

## What Is a Cybersecurity Clinic?

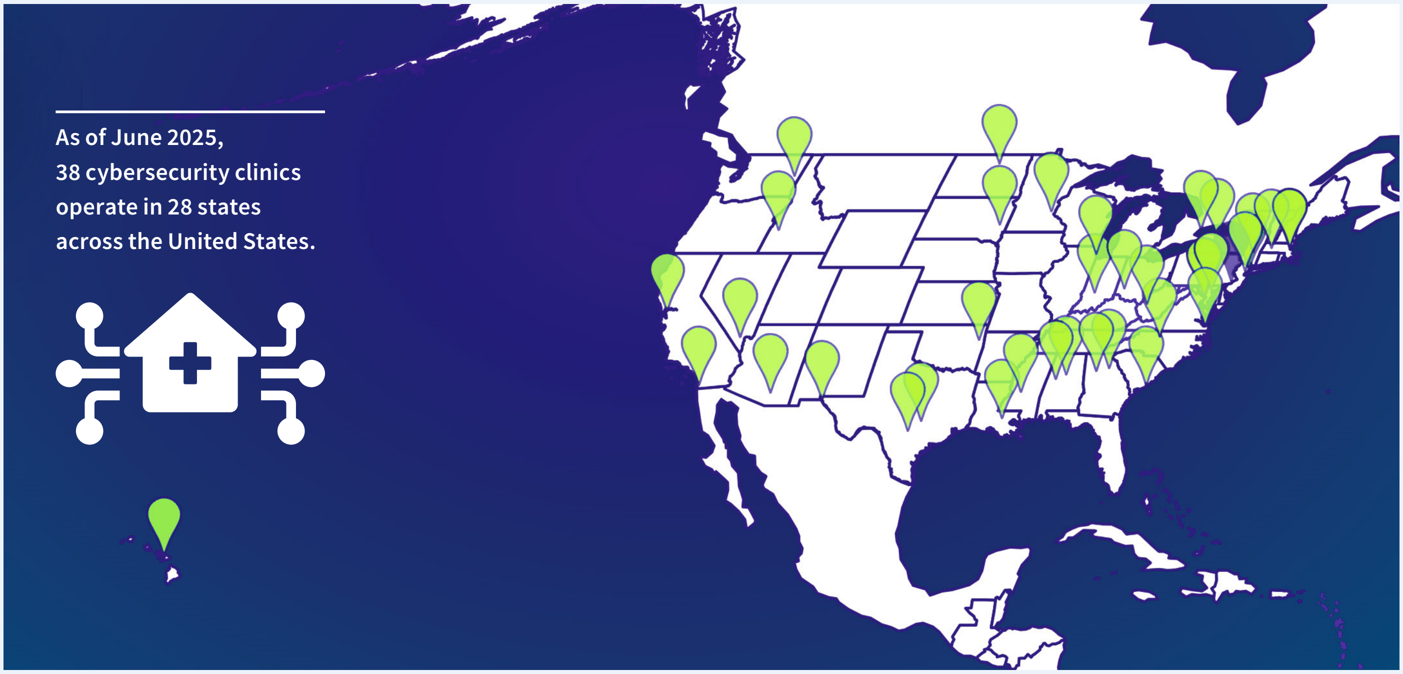
Modeled after legal and medical school clinics, cybersecurity clinics train students at colleges and universities to provide pro bono cybersecurity services to community organizations, including small businesses, nonprofits, cities and towns, rural school districts, small utilities, and others.

Cybersecurity clinics offer students from diverse backgrounds and degree paths real-world experience, while also providing a source of free cybersecurity assistance to organizations that would otherwise be unable to afford these services. Clinics serve as a skills-based learning environment for students and as a vital local resource for improving the cybersecurity resilience of communities.

## What Is The Current Scale Of Cybersecurity Clinics?

- According to the Consortium of Cybersecurity Clinics,[75] as of June 2025, 33 cybersecurity clinics operate in at least 28 states in the U.S., with a total of over 50 clinics worldwide.
- Clinics have trained over 1500 students to provide pro bono cybersecurity risk assessments.
- Clinics have provided free assistance to over 150 community organizations, including nonprofits, cities, healthcare organizations, schools, and more.

**Figure 7: Cybersecurity Clinics in the U.S.** (Source: The Consortium of Cybersecurity Clinics)



## Why are Cybersecurity Clinics an Important Part of The Solution?

University-based cybersecurity clinics help clients develop long-term cybersecurity defense, increase their resilience, and expand their cybersecurity capacity. Students provide a range of digital security services, such as vulnerability and risk assessments, cybersecurity policy templates, incident response plans, ransomware training, NIST and CMMC certifications, and more.

There is no substitute for face-to-face discussions in building lasting cyber resilience, but many community organizations cannot afford costly professional consulting services. Cybersecurity clinics fill this gap by providing proactive assessments to organizations that are currently underserved by the cyber market.

## Student and Regional SOCs: A Growing Detection Service

Student-staffed security operations centers (SOCs) are growing higher-education-based cyber defense programs. These innovative centers offer monitoring, detection, and, in some cases, incident response services to community organizations. Often partnering with private-sector entities for tools, institutes of higher education train students to take shifts at these industry-standard labs to monitor network traffic and escalate potentially malicious activity for investigation.

Student SOCs can create wide-ranging partnerships; Texas[76] and Louisiana[77] both invested in regional SOCs, which include partnerships with the state National Guard, state emergency management, and state police, while training students for cyber analyst jobs. Student SOCs are promising models for student cybersecurity training and the cyber defense of community organizations.

## Case Study

**The Challenge:** A Municipal Water District in southern California provided critical water and wastewater treatment to nearby residents. They contacted the San Diego Cyber Clinic to strengthen their cyber defenses amid a surge in cyber attacks on water utilities and the pre-positioning of malicious actors on IT networks in critical infrastructure.

**The Cyber Clinic Response:** A team of five students from the San Diego Cyber Clinic performed several free services for the water district, including a comprehensive cybersecurity assessment of their implementation of key protections. The students also conducted a penetration test, a phishing test, and a social engineering test to develop a holistic view of the water district's defensive abilities.

**Outcomes:** From these assessments, the students learned that the water district had a gap in policies they could rely on in the event of an emergency. They developed and customized this essential documentation for the water district, including an Incident Response Plan, Disaster Recovery Plan, and a Business Continuity Plan (BCP). The students also provided an overview of the results of their assessment, penetration, and phishing tests so that the water district could improve. By integrating these components, the project not only uncovered risks but also provided a roadmap for the district to enhance its resilience against cyber threats.

# State Civilian Cyber Corps

## What is a State Civilian Cyber Corps?

A civilian cyber corps is a team of cybersecurity professionals who volunteer to provide preventive and reactive cybersecurity services to designated beneficiaries. State civilian cyber corps operate under the authority of a state government department or agency. They typically offer services that include: (1) education and training; (2) vulnerability and risk assessments; and (3) on-call expertise, incident response, and recovery efforts.

Civilian cyber corps can provide several benefits to states, including:

- Reducing the costs of cybersecurity incidents to governments and taxpayers by increasing awareness, supporting prevention, and helping to contain incidents;
- Improving a state's cyber resilience by delivering education and training to beneficiaries and identifying vulnerabilities, risks, and remediation recommendations, and providing a resource for states to provide surge support in the event of a regional or statewide cyber emergency;
- Growing and enhancing a state's cybersecurity workforce, while helping to fill the workforce gap faced by SLTTs and SMBs; and
- Providing a hub for community and civic engagement on cybersecurity by facilitating awareness and technical training/workforce enhancement, and by providing a credible civilian connection to governmental institutions.

## What is the Current Scale of State Civilian Cyber Corps?

Six states have active civilian cyber corps,[78] which together have over 900 volunteers.[79]

- Louisiana[80]
- Maryland[81]
- Michigan[82]
- Ohio[83]
- Texas[84]
- Wisconsin[85]

Two states are in the process of forming civilian cyber corps:

- New Jersey
- Oklahoma[86]

## Why are State Civilian Cyber Corps an Important Part of the Solution?

States with civilian cyber corps have utilized them to provide cybersecurity awareness training to nonprofit organizations and schools, conduct risk assessments for government and critical infrastructure organizations, and assist in responding to cybersecurity incidents. Civilian cyber corps have responded to numerous cyberattacks in multiple states; however, the effectiveness of state cyber corps extends well beyond incident response. State cyber corps can provide incident post-mortems, including monitoring and detection, thereby increasing the cyber resilience of community organizations even after an attack has occurred.

# Case Study

**What Happened?** A ransomware group attacked a Wisconsin county government, destroying the entire network infrastructure and all data backups. With the exception of a few terabytes of departmental data, the county lost a significant amount of service data.

**The Cyber Corps Response:** The Wisconsin Cyber Response Team, operating under the Wisconsin Department of Emergency Management, mobilized a small team of volunteers to arrive on-site, assess the situation, and develop a course of action with the network owner and the cyber insurance company.

The Wisconsin Cyber Response Team performed immediate actions to contain the attack and began obtaining random-access memory (RAM) and drive images, Kroll Artifact Parser and Extractor (KAPE) captures, and logs to preserve as much forensic data as possible. Working in collaboration with a third-party digital forensics and incident response (DFIR) vendor, remote members of the Wisconsin Cyber Response Team continued to perform data forensics analysis to confirm the data integrity of compromised data backups, identify an attack timeline, and provide additional analytical support while the on-site team developed a support plan with the network owner and DFIR vendor.

Given the likely scope of the county's data loss, the Wisconsin Cyber Response Team also assisted the network owner's efforts with:

- Fully implementing multi-factor authentication with a newly de-federated M365 environment, a key control in preventing unauthorized access to sensitive data;
- Migrating county users to a new domain controller, and creating strong passwords, further protecting accounts from unauthorized use;
- Leveraging the inherent security of the M365 environment to leverage Microsoft SharePoint as a de facto file server for the county's departments, improving protections for sensitive data;
- Configuring CISCO High-Power switches with updated security control configurations; and
- Creating a new ESXi network infrastructure with segmented immutable backups.

**Outcome:** The Wisconsin Cyber Response Team continued to support the county in conducting a post-mortem analysis, including by providing an initial round of cybersecurity assessments using CISA's CSET protocol, with the intention for the network owner to further harden the network based on the assessment findings.

- Wisconsin Emergency Management officials continued to engage with the county's emergency management director to collaborate with the IT director on developing an incident response plan. This plan included a maintenance schedule, annual assessments, and training.
- Emergency Management officials continued to provide awareness training for county department heads and elected officials in the form of table-top and functional exercises.
- The Wisconsin CRT performed a second round of cybersecurity assessments using the CSET protocol for additional security hardening and incident response planning.
- A two-week penetration test engagement was conducted following the second-round hardening to provide the network owner with additional findings and establish opportunities for further hardening, thereby providing reasonable assurance that the county's network conditions would establish a new security baseline.

One of the most significant outcomes of this engagement was the establishment and development of deeper interpersonal and state-to-county relationships. The Wisconsin Cyber Response Team's enduring relationships with county officials over the "long haul" have reinforced that the team's commitment to serving local communities as "cyber fiduciaries" was not hyperbole or lip service. The Wisconsin Cyber Response Team views each incident as an opportunity to serve and support entities that require a high level of cybersecurity expertise but cannot afford to invest in such resources.

# Nonprofit Volunteering Groups

## What is a Nonprofit Cyber Volunteering Group?

A nonprofit cyber volunteering group is an organization, typically registered as a 501(c)(3) or its equivalent, that provides free or at-cost cyber resilience services to under-resourced communities, including other nonprofits, hospitals, public interest organizations, and other at-risk organizations that lack cybersecurity expertise. These groups play a crucial role in narrowing the cybersecurity gap by offering services such as risk assessments, cyber hygiene training, and incident response. Some examples of nonprofit cyber volunteering groups are: Apparo, the Center for Cyber Safety and Education, CR-ISAC, CTI League, CyberPeace Builders, and DEF CON Franklin.

## What is the Current Scale of Nonprofit Cyber Volunteering Groups?

Nonprofit cybersecurity volunteer groups help a few hundred beneficiaries in the United States each year. They count thousands of members and represent the majority of cyber volunteers in the U.S. Often operating nationwide, they draw talent from diverse backgrounds: private-sector professionals, veterans, certified experts, and others. Nonprofit cyber volunteering groups represent an excellent opportunity to scale up cyber civil defense, as there are approximately 1.2 million active cybersecurity professionals in the U.S., many of whom may be willing to contribute a few hours each year to support their communities.

## Why are Nonprofit Cyber Volunteering Groups an Important Part of the Solution?

Cyber nonprofit volunteering groups have proven to be effective in multiple, context-specific ways. First, these groups are uniquely positioned because of their mission-first orientation. Their focus on service rather than profit means they are often more patient, culturally aware, and tailored in their approach than large enterprise security vendors.

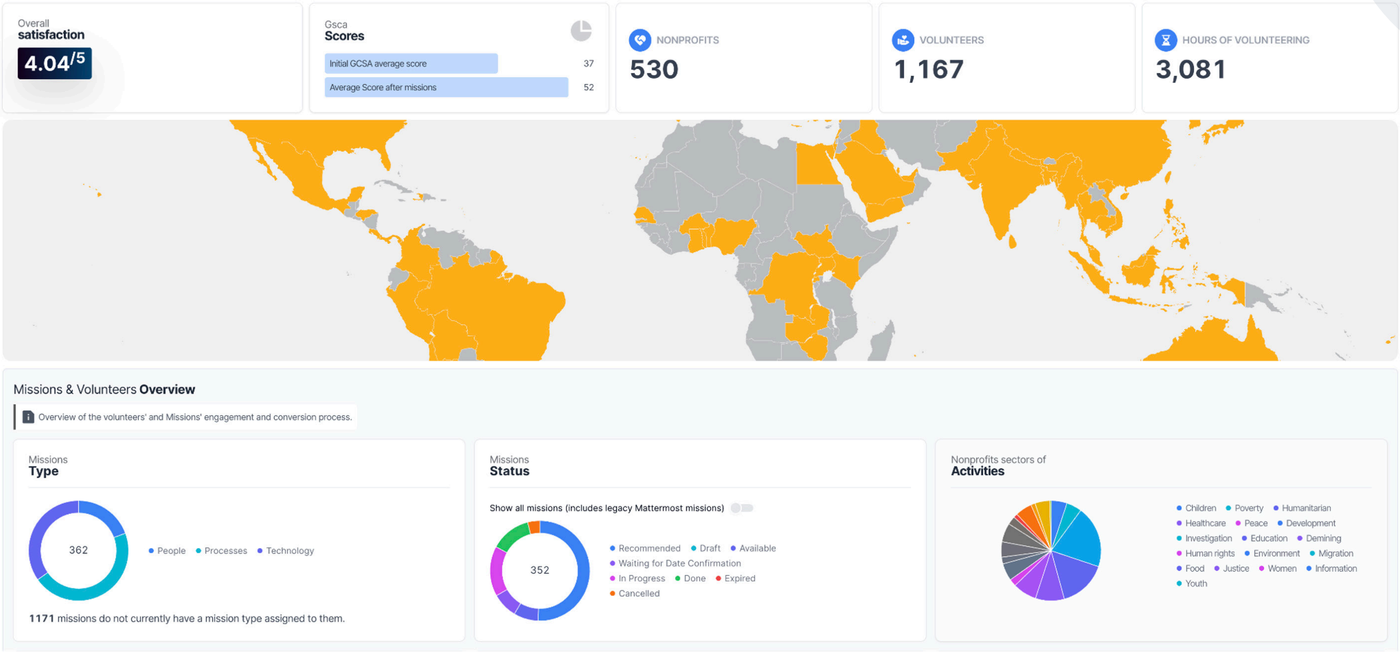
Second, due to frequent funding constraints, they often innovate out of necessity. Lacking the resources of commercial firms, they develop creative, scalable, and lightweight solutions — sometimes even open-source or community-built tools — to meet the needs of their beneficiaries. They adapt quickly to new threat environments and have honed the ability to prioritize the security interventions that matter most.

Third, nonprofit cyber volunteer groups are not monolithic. They fill various needs. Some choose to focus on intimate, community cohorts. Others work to scale and reach broad beneficiary networks. Some offer unique expertise, such as healthcare cybersecurity, and others leverage unique partnerships with public authorities and industry.

Lastly, although the sector lacks a framework for measuring impact, several indicators of success are used by various groups, including documented improvement in cybersecurity posture (e.g., pre- and post-assessments), beneficiary satisfaction and testimonials, and evidence of community building.

For example, during a 2024 pilot with the NGO-ISAC, the CyberPeace Builders supported 45 U.S.-based, democracy-focused nonprofits. Entry and exit cybersecurity assessments were conducted, showing that 100% of participating organizations improved their cybersecurity posture over the course of the program, demonstrating a positive impact.

**Figure 8: CyberPeace Builders Overview** (Source: The CyberPeace Builders)



Overall satisfaction

4.04/5

Gsca Scores

| | |
|---|---|
| Initial GCSA average score | 37 |
| Average Score after missions | 52 |

NONPROFITS 530

VOLUNTEERS 1,167

HOURS OF VOLUNTEERING 3,081

Missions & Volunteers **Overview**

Overview of the volunteers' and Missions' engagement and conversion process.

Missions **Type**

**1171** missions do not currently have a mission type assigned to them.

Missions **Status**

Show all missions (includes legacy Mattermost missions)

Nonprofits sectors of **Activities**

## Case Study

The CyberPeace Builders is a volunteer program hosted by the CyberPeace Institute, an international nonprofit organization. The program bridges the cybersecurity gap for under-resourced organizations by mobilizing a vetted network of over 1,400 cybersecurity professionals from the private sector. These volunteers offer structured, pro bono support to NGOs worldwide, including risk assessments, tailored recommendations, staff training, policy templates, threat alerts, and more.

What makes the CyberPeace Builders model particularly innovative is its ability to meet two distinct needs at once: companies seeking to attract, retain, and engage top cyber talent through purpose-driven work, and NGOs in urgent need of trusted cybersecurity support. CyberPeace Builders demonstrates how cross-sector collaboration, standardized processes, and volunteer expertise can help protect civil society organizations at scale.

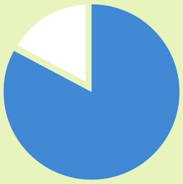
**Challenge:** As a small, U.S.-based nonprofit organization providing essential HIV-related services, AIDS Resource faced significant cybersecurity challenges. Limited funding and capacity often meant that cybersecurity took a backseat, despite the fact that the nonprofit's work made them a target for malicious actors. Without dedicated resources, the organization was vulnerable; they were aware they needed better support to protect their staff, data, and community.

**Solution:** In 2022, AIDS Resource joined the CyberPeace Builders program with a baseline cybersecurity score of just 37%. Recognizing the urgent need for support, the CyberPeace Institute mobilized its network of expert volunteers to guide the NGO through practical and targeted cybersecurity improvements.

**Outcomes:** To date, AIDS Resource has completed 19 cybersecurity missions and received over 48 hours of hands-on support from cybersecurity experts from various companies. Their cybersecurity assessment score has soared to 83% — a 46 percentage point improvement — reflecting a stronger and more resilient cybersecurity posture. Most importantly, their team is now far more aware, confident, and equipped to defend against the cyber threats they face.

**GCSA Score**

84% +46% since first assessment



**Volunteering hours received**

48h +90% since last year

**In-kind equivalent received**

$72,000 +$13,500 since last year

**Missions completed**

19

# Strengthen the Regional Cyber Support Ecosystem

States can play a pivotal role in launching and scaling cyber volunteer groups by funding ambitious initiatives with higher education, establishing state cyber corps, and developing structured pathways for private-sector volunteering.

### 1. Fund Ambitious Initiatives with Higher Education

▶ States can fund cyber clinics. As one pathway, states can incorporate cyber clinics into their state cyber plan, and utilize funds from DHS State and Local Cybersecurity Grants (SLCGP), as available, to provide cyber services to local governments in a manner that benefits the state in the long term.

To help guide these investments, the Consortium of Cybersecurity Clinics has developed a Clinic Development Toolkit with step-by-step information on how to start a clinic, including startup cost estimates. The Consortium also meets virtually once a month, allowing dozens of current and developing clinics to share best practices and resources.

▶ States can fund Student SOC programs. Student security operations centers (SOCs) present states with an opportunity to invest in monitoring and detection services for community organizations while training students for cyber jobs. Texas and Louisiana both invested in regional SOCs to protect local governments and K-12 schools, respectively. Students staff the SOCs and work in partnership with local universities, state emergency management agencies, state National Guard, and corporate partners.

▶ States can fund higher-ed research partnerships. Long-term public-private partnerships enable the sharing of comprehensive information about successes and gaps at the local level, allowing states to make more effective investments in community cybersecurity. Indiana's CyberTrack partnership,[87] for example, is bringing together leading universities to assess all municipalities in the state, to conduct 342 cybersecurity assessments over four years, and provide continual updates on findings to state leaders.

### 2. Create Authorities for State Civilian Cyber Corps

▶ States can create new legislative or executive authorities for state civilian cyber corps. Civilian cyber corps can be a valuable resource for helping states increase the cyber preparedness of community organizations. State governments can help launch civilian cyber corps by forming a volunteer cyber reserve organization pursuant to new or existing legislative or executive authorities.

▶ The biggest hurdle to establishing a new civilian cyber corps program lies in obtaining the necessary legislative or executive authority to create one from the appropriate state entity. This can be accomplished by using the Civilian Cyber Corps Model Law.[88] States can also refer to additional resources on state cyber corps programs.[89,90]

### 3. Structure Pathways for Private-Sector Volunteering

▶ States can incentivize companies to provide skilled volunteers. States can encourage private companies to contribute volunteers, tools, and threat intelligence to nonprofits, including by offering tax incentives or other benefits to companies that actively participate in cyber volunteering initiatives.

▶ States can endorse and collaborate with local volunteering groups. State endorsement of nonprofit and corporate volunteering programs can help attract additional volunteers, clients, and funders. States can also partner with local volunteer organizations to support specific regions or types of organizations.

# Conclusion

The status quo — in which community organizations are expected to shoulder the entire burden of cybersecurity themselves — cannot continue, nor can we accept a future where cybercriminals frequently shut down critical community organizations, such as schools, utilities, hospitals, and other essential services. But there is a path forward by which cyber leaders at the regional level, from universities to nonprofits to state governments, band together to create local ecosystems of cyber support.

We propose a co-responsibility model for cybersecurity that equitably distributes duties between individual organizations and more capable organizations, including governments and enterprise businesses.

The groundwork for this new pathway already exists. Cyber volunteering programs have already emerged across the country that enlist thousands of volunteers and provide free services and low-cost tools to community organizations. We must significantly scale these programs in the short term to cover regional and sectoral gaps in critical services. This report provides actionable recommendations for an “on-ramp” to scale short-term aid through cyber volunteering.

In the long term, we must also shift the balance of responsibility away from community organizations, not by expecting every organization to hire a full-time cybersecurity team, but by simplifying cybersecurity for non-experts and strategically leveraging pools of resident experts in MSPs, MSSPs, cyber volunteering groups, and enterprise businesses.

The role of states is also greatly increasing in community cybersecurity. We produced a guidebook for state government leaders to create local ecosystems of cyber support through investing in academic partnerships like cyber clinics and student SOCs, creating authorities for civilian cyber corps, and bolstering nonprofit volunteering programs. The guidebook features applied case studies and model legislation, where available, to facilitate adoption of our recommendations

The Cyber Resilience Corps, co-chaired by the UC Berkeley Center for Long-Term Cybersecurity and the CyberPeace Institute, looks forward to tackling the challenges of volunteer coordination and scale in the next phase of this initiative. We hope this report will inspire our fellow leaders to take action — to invest not only in sectors but in entire communities — and to play their unique part in this cooperative journey toward a just and secure prosperous future.

# Acknowledgments

On behalf of CLTC, we would like to thank members of the Cyber Resilience Corps for their generous time, input, and support of this project. Without their deep, lived expertise in cybersecurity for under-resourced organizations, none of this work would be possible.

## Cyber Resilience Corps Co-Chairs

| | |
|---|---|
| **Sarah Powazek** | UC Berkeley CLTC |
| **Grace Menna** | UC Berkeley CLTC |
| **Ann Cleaveland** | UC Berkeley CLTC |
| **Adrien Ogée** | CyberPeace Institute |
| **Jessica Walton** | CyberPeace Institute |
| **Stéphane Duguin** | CyberPeace Institute |

## Cyber Resilience Corps Members

| | |
|---|---|
| **Alisha Wenc** | Center for Cyber Safety and Education |
| **Amanda Bennett** | Personified |
| **Ashleigh Pratt** | Techies for Reproductive Justice |
| **Elijah Baucom** | UC Berkeley Cybersecurity Clinic |
| **Eric Franco** | Wisconsin Emergency Management |
| **Fabien Leimgruber** | CyberPeace Builders |
| **Francesca Lockhart** | UT Austin Strauss Center for International Security and Law |
| **Jake Braun** | DEF CON Franklin |
| **Jessica Davenport** | National Governors Association |
| **Joshua Corman** | UnDisruptable27 at Institute for Security + Technology (IST) |
| **Kelley Misata** | Sightline Security |
| **Lance Larson** | San Diego Cyber Clinic |
| **Laura Mateczun** | University of Maryland, Baltimore |
| | County Cybersecurity Clinic |
| **MAJ (MD) Jeremy O'Mard** | Maryland Defense Force |
| **Mark Bell** | Ohio Cyber Range |
| **Matthew Grote** | Cybersecurity and Infrastructure Security Agency (CISA) |
| **Michael Razeeq** | UC Berkeley CLTC |
| **Natalie Sjelin** | CIAS Community Cybersecurity Clinic (C4) at UTSA |
| **Paul Chang** | DEF CON Franklin |
| **Ray Davidson** | Independent Researcher |
| **Steve Sharer** | RipRap Security |
| **Tazin Khan** | Cyber Collective |
| **Thom Kaye** | Access Now |
| **Tim Ball** | Independent Researcher |
| **Vic Macias** | Civilian Reserve ISAC |

**We would like to thank other individuals whose time made this report better:**

**Mark E. Schreiber**, **Brian Long**, and **James Mann** from McDermott Will & Emery LLP, in addition to **Richard Stiennon** from IT Harvest.

We would also like additional members of the CLTC team for their contributions to the report: **Chuck Kapelke** and **Shannon Pierson**.

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.

# References

1. Consortium of Cybersecurity Clinics. https://cybersecurityclinics.org/.

2. Cyber Volunteer Resource Center | CISA. https://www.cisa.gov/audiences/high-risk-communities/cybervolunteerresourcecenter.

3. Cyber Resilience Corps (CRC) members listed in the Acknowledgments Section

4. Harry, Charles, et al. “Measuring the Size and Severity of the Integrated Cyber Attack Surface across US County Governments.” *Journal of Cybersecurity, vol. 11, no. 1, Jan. 2025, p. tyae032. Silverchair,* licensed under CC BY-NC-ND . https://doi.org/10.1093/cybsec/tyae032.

5. *The State of Ransomware in Healthcare 2024 – Sophos Partner News.* https://partnernews.sophos.com/en-us/2024/08/resources/the-state-of-ransomware-in-healthcare-2024/.

6. Moody, Rebecca. “Ransomware Roundup: Q1 2025.” Comparitech, 8 Apr. 2025, https://www.comparitech.com/news/ransomware-roundup-q1-2025/.

7. CyberPeace Tracer (Focus on CSOs in the US), CyberPeace Institute. https://cyberpeacetracer.ngo/us .

8. 2024 Ransomware Report: Sophos State of Ransomware. https://www.sophos.com/en-us/content/state-of-ransomware.

9. Dareen, Seher and Vallari Srivastava. “Cyberattacks on US Utilities Surged 70% This Year, Says Check Point” | Reuters, 11 Sept. 2024, https://www.reuters.com/technology/cybersecurity/cyberattacks-us-utilities-surged-70-this-year-says-check-point-2024-09-11/.

10. SNAP Replacement of Stolen Benefits Dashboard | Food and Nutrition Service. https://www.fns.usda.gov/data-research/data-visualization/snap-replacement-stolen-benefits-dashboard.

11. “‘They’re Stealing Food from My Kids’: SNAP Recipients and the Struggle against EBT Theft.” Propel, 20 May 2024, https://www.propel.app/insights/theyre-stealing-food-from-my-kids-snap-recipients-and-the-struggle-against-ebt-theft/.

12. Greig, Jonathan. “Ransomware Attack on New York Blood Center Forces Workarounds, Drive Cancellations.” Cyber Security News | The Record, The Record, 30 Jan. 2025, https://therecord.media/ransomware-attack-new-york-blood-center-forces-workarounds.

13. Quraishi, Ash-har, Ari Sen, Scott Pham, Amy Corral, and Taylor Johnston. “Ransomware Attacks on Schools Threaten Student Data Nationwide” - CBS News. 26 Aug. 2024, https://www.cbsnews.com/news/school-ransomware-attacks-threaten-student-data/.

14. Morgan, Steve. “2024 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics.” Cybercrime Magazine, 24 June 2024, https://cybersecurityventures.com/cybersecurity-almanac-2024/.

15. Nather, Wendy. “T1R Insight: Living below the Security Poverty Line.” 451 Research, 26 May 2011, https://web.archive.org/web/20140203193523/https:/451research.com/t1r-insight-living-below-the-security-poverty-line.

16. “Information Security Analysts.” Bureau of Labor Statistics, https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.

17. Understanding Nonprofit Salaries: A Comprehensive Guide | Charity Charge. 20 June 2024, https://www.charitycharge.com/nonprofit-resources/nonprofit-salaries/.

18. How Much Do Managed Cybersecurity Services Cost? | VC3. https://www.vc3.com/blog/managed-cyber-security-services-cost.

19. “2024 Security Budget Benchmark Report: Key Findings.” IANS, https://www.iansresearch.com/resources/all-blogs/post/security-blog/2024/09/05/2024-security-budget-benchmark-report--key-findings.

20. 94% of respondents had a revenue of over $100M, with most revenue over $1B

21. “Nonprofit Impact Matters.” National Council of Nonprofits, https://www.nonprofitimpactmatters.org/data/downloadable-charts/.

**22.** 92% of nonprofits have budgets of $1M or less per year, and 88% have a budget of less than $500,000

**23.** "CyberPeace Analytical Report: - NGOs Serving Humanity at Risk: Cyber Threats Affecting 'International Geneva.'" CyberPeace Institute, 2023, https://geneva.cyberpeace.ngo/.

**24.** Powazek, Sarah, and Shannon Pierson. "CyberCAN: Cybersecurity for Cities and Nonprofits." UC Berkeley Center for Long-Term Cybersecurity. Nov 2024, https://cltc.berkeley.edu/publication/cybercan-cybersecurity-for-cities-and-nonprofits/.

**25.** Data pulled from IT Harvest Database, https://it-harvest.com/.

**26.** Healey, Jason, et al. "Understanding Cyber Market Failures." Lawfare, Apr. 2025. www.lawfaremedia.org, https://www.lawfaremedia.org/article/understanding-cyber-market-failures.

**27.** "K-12 Cybersecurity Guidebook." Google for Education, 2023. https://services.google.com/fh/files/misc/k12cybersecurityguide.pdf.

**28.** Upadhyay, Mayank. "Mandatory MFA Is Coming to Google Cloud. Here's What You Need to Know." Google Cloud Blog, 4 Nov. 2024, https://cloud.google.com/blog/products/identity-security/mandatory-mfa-is-coming-to-google-cloud-heres-what-you-need-to-know.

**29.** "Plan for Mandatory Microsoft Entra Multifactor Authentication (MFA) for Azure other admin portals" - Microsoft Entra ID. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mandatory-multifactor-authentication.

**30.** Rural and Municipal Utilities Play Critical Role in America's Energy Security | Department of Energy. 21 Dec. 2022, https://www.energy.gov/ceser/articles/rural-and-municipal-utilities-play-critical-role-americas-energy-security.

**31.** Barry, Ellen, and Nicole Perlroth. "Patients of a Vermont Hospital Are Left 'in the Dark' After a Cyberattack." The New York Times, 26 Nov. 2020. NYTimes.com, https://www.nytimes.com/2020/11/26/us/hospital-cyber-attack.html.

**32.** Collier, Kevin. "An Illinois Hospital Is the First Health Care Facility to Link Its Closing to a Ransomware Attack." NBC News, 12 June 2023, https://www.nbcnews.com/tech/security/illinois-hospital-links-closure-ransomware-attack-rcna85983.

**33.** "Rural Hospital Closures." University of North Carolina at Chapel Hill Sheps Center, https://www.shepscenter.unc.edu/programs-projects/rural-health/rural-hospital-closures/.

**34.** Faulk, Lewis, et al. Nonprofit Trends and Impacts 2021: National Findings on Donation Trends from 2015 through 2020, Diversity and Representation, and First-Year Impacts of the COVID-19 Pandemic. https://www.urban.org/sites/default/files/publication/104889/nonprofit-trends-and-impacts-2021_2.pdf.

**35.** Nonmetro Poverty Rates Remain Higher than Metro | Economic Research Service. https://www.ers.usda.gov/data-products/chart-gallery/chart-detail?chartId=58300.

**36.** "Rural and Municipal Utilities Play Critical Role in America's Energy Security." Energy.Gov. 21 Dec. 2022, https://www.energy.gov/ceser/articles/rural-and-municipal-utilities-play-critical-role-americas-energy-security.

**37.** Schaeffer, Katherine. "U.S. Public, Private and Charter Schools in 5 Charts." Pew Research Center, 6 June 2024, https://www.pewresearch.org/short-reads/2024/06/06/us-public-private-and-charter-schools-in-5-charts/.

**38.** The NCES Fast Facts Tool Provides Quick Answers to Many Education Questions (National Center for Education Statistics). National Center for Education Statistics, https://nces.ed.gov/fastfacts/display.asp?id=372.

**39.** Rural Health Services | American Hospital Association. https://www.aha.org/advocacy/rural-health-services.

**40.** Michigan Cyber Civilian Corps (MiC3). https://www.michigan.gov/dtmb/services/cybersecurity/michigan-cyber-civilian-corps-mic3.

**41.** Wisconsin Cyber Response Team | Wisconsin Emergency Management. https://wem.wi.gov/wisconsin-cyber-response-team/.

**42.** Texas Volunteer Incident Response Team (VIRT) | Texas Department of Information Resources. https://dir.texas.gov/information-security/cybersecurity-incident-management-and-reporting/texas-volunteer-incident.

**43.** Maryland Defense Force. https://md.mddf.us/.

**44.** OhCR - Ohio Cyber Reserve. https://ohcr.ohio.gov/.

**45.** Razeeq, Michael. "Civilian Cyber Corps: A Model Law for States." New America. 26 Sept 2024, http://newamerica.org/future-security/reports/civilian-cyber-corps-a-model-law-for-states/.

**46.** "La. Guard Announces Stationing of the 178th Cyber Protection Team at Cyber Innovation Center in Bossier" – Louisiana National Guard. https://geauxguard.la.gov/la-guard-announces-stationing-of-the-178th-cyber-protection-team-at-cyber-innovation-center-in-bossier/.

**47.** CyberPeace Builders, Cyberpeace Institute. https://www.cpb.ngo.

**48.** Zaidenberg, Ohad. Global Volunteer Cyberthreat Community-CERT | CTI League. 9 Apr. 2020, https://cti-league.com/.

**49.** DEF CON Franklin. https://defconfranklin.com/.

**50.** "Cyberlaw Clinic." Harvard Law School, https://hls.harvard.edu/clinics/in-house-clinics/cyberlaw-clinic/.

**51.** Consortium of Cybersecurity Clinics. https://cybersecurityclinics.org/.

**52.** "Apparo | Amplifying Nonprofit Impact." Apparo, https://apparo.org/.

**53.** CyberPeace Builders, Cyberpeace Institute. https://www.cpb.ngo.

**54.** State, Local, Tribal, and Territorial Government | Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/audiences/state-local-tribal-and-territorial-government.

**55.** Franco, Eric. Zoom Interview, 24 Jan. 2025.

**56.** Collection of interviews with representatives of numerous MSPs.

**57.** Welcome to InfraGard — Site. https://www.infragard.org.

**58.** State, Local, Tribal & Territorial Indicators of Compromise Automation Pilot Fact Sheet | CISA. 14 July 2021, https://www.cisa.gov/resources-tools/resources/state-local-tribal-territorial-indicators-compromise-automation-pilot.

**59.** Wood, Colin. "MS-ISAC Loses Federal Support for Threat Intelligence, Incident Response." StateScoop, 11 Mar. 2025, https://statescoop.com/ms-isac-loses-federal-support/.

**60.** Cyber Volunteer Resource Center | CISA. https://www.cisa.gov/audiences/high-risk-communities/cybervolunteerresourcecenter.

**61.** "Creating a Cyber Volunteer Force: Strategy and Options | PDF." McDermott Will & Emery, March 2023, https://www.mwe.com/pdf/creating-a-cyber-volunteer-force-strategy-and-options/.

**62.** Greig, Jonathan. "CISA Cuts $10 Million Annually from ISAC Funding for States amid Wider Cyber Cuts." Cyber Security News | The Record, The Record, 12 Mar. 2025, https://therecord.media/cisa-cuts-10-million-isac-funding.

**63.** Wood, Colin. "Nonprofit to Provide Gap Funding for MS-ISAC Cuts." StateScoop, 8 Apr. 2025, https://statescoop.com/ms-isac-funding-cuts-services-continue-2025/.

**64.** Beckman, Joe, Craig Jackson, and Ranson Ricks. "Cybertrack Report: Aggregate Results & Analysis from 76 Assessments (May 2023 - May 2024)." Indiana's Local Government Cybersecurity Assessment Program. Jun. 2024, https://incybertrack.org/media/qtpkba0q/cybertrack-aggregate-results-report-june-2024.pdf.

**65.** Data sourced from IT Harvest, https://it-harvest.com/.

**66.** "National Cybersecurity Strategy | ONCD." The White House, 2 Mar. 2023, https://bidenwhitehouse.archives.gov/oncd/national-cybersecurity-strategy/.

**67.** Powazek, Sarah, and Shannon Pierson. "CyberCAN: Cybersecurity for Cities and Nonprofits." UC Berkeley Center for Long-Term Cybersecurity. Nov 2024, https://cltc.berkeley.edu/publication/cybercan-cybersecurity-for-cities-and-nonprofits/.

**68.** Beckman, Joe, Craig Jackson, and Ranson Ricks. "Cybertrack Report: Aggregate Results & Analysis from 76 Assessments (May 2023 - May 2024)." Indiana's Local Government Cybersecurity Assessment Program. Jun. 2024, https://incybertrack.org/media/qtpkba0q/cybertrack-aggregate-results-report-june-2024.pdf.

**69.** Indiana Cybertrack. https://incybertrack.org/.

**70.** Federal and state laws about volunteering and indemnity can be found in the Volunteer Protection Act and are summarized here and here.

**71.** Template model agreements of this sort can be found here (App. 3, pp. 53-62). It is important in these agreements to define the scope of volunteer work and expectations, especially in distinguishing proactive cyber assessment work from incident response. Capabilities and qualifications in these two areas differ markedly.

**72.** Sen. Burr, Richard [R-NC. S.754 - 114th Congress (2015-2016): An Act to Improve Cybersecurity in the United States through Enhanced Sharing of Information about Cybersecurity Threats, and for Other Purposes. 28 Oct. 2015, https://www.congress.gov/bill/114th-congress/senate-bill/754. 2015-03-17.

**73.** Secure Your Products | CISA. https://www.cisa.gov/secure-our-world/secure-your-products.

**74.** Consortium of Cybersecurity Clinics. https://cybersecurityclinics.org/.

**75.** Orders, Executive. “Achieving Efficiency Through State and Local Preparedness.” The White House, 19 Mar. 2025, https://www.whitehouse.gov/presidential-actions/2025/03/achieving-efficiency-through-state-and-local-preparedness/.

**76.** AAlaniz, Amanda. “New Regional Security Operations Center Opens at UTRGV to Enhance Cybersecurity for the Region”. UTRGV, 14 Nov. 2024. https://www.utrgv.edu/newsroom/2024/11/14/boosting-cybersecurity-efforts.htm.

**77.** “Louisiana Enables Cyber Protection for Higher Ed in the State Through LSU”. https://www.lsu.edu/mediacenter/news/2023/09/wfl-soc.php.

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

**79.** Razeeq, Michael. “Civilian Cyber Corps: A Model Law for States.” New America. 26 Sept 2024, http://newamerica.org/future-security/reports/civilian-cyber-corps-a-model-law-for-states/.

**80.** State Guard – Louisiana National Guard. https://geauxguard.la.gov/state-guard/.

**81.** Maryland Defense Force. https://md.mddf.us/.

**82.** Michigan Cyber Civilian Corps (MiC3). https://www.michigan.gov/dtmb/services/cybersecurity/michigan-cyber-civilian-corps-mic3.

**83.** OhCR - Ohio Cyber Reserve. https://ohcr.ohio.gov/.

**84.** Texas Volunteer Incident Response Team (VIRT) | Texas Department of Information Resources. https://dir.texas.gov/information-security/cybersecurity-incident-management-and-reporting/texas-volunteer-incident.

**85.** Wisconsin Cyber Response Team | Wisconsin Emergency Management. https://wem.wi.gov/wisconsin-cyber-response-team/.

**86.** “Cybersecurity.” Oklahoma Office of Homeland Security, https://oklahoma.gov/homeland-security/cyber-security.html.

**87.** Indiana Cybertrack. https://incybertrack.org/.

**88.** Razeeq, Michael. “Civilian Cyber Corps: A Model Law for States.” New America. 26 Sept 2024, http://newamerica.org/future-security/reports/civilian-cyber-corps-a-model-law-for-states/.

**89.** “Creating a Cyber Volunteer Force: Strategy and Options | PDF.” McDermott Will & Emery, March 2023, https://www.mwe.com/pdf/creating-a-cyber-volunteer-force-strategy-and-options/.

**90.** Association, National Governors. “Re-Envisioning State Cyber Response Capabilities: The Role of Volunteers in Strengthening Our Systems.” National Governors Association, 16 June 2022, https://www.nga.org/publications/re-envisioning-state-cyber-response-capabilities-the-role-of-volunteers-in-strengthening-our-systems/.

CYBER RESILIENCE CORPS
USA

**For more information:**

www.cybervolunteers.us
https://cltc.berkeley.edu/program/cyber-resilience-corps
cltc@berkeley.edu