Bridging Digital Divides:

Expanding Cybersecurity in Underserved Communities

November 2024

NASCIO®
Representing Chief Information
Officers of the States

Introduction

As the world continues to become “digital by default,” cybersecurity has become a major concern for individuals, organizations and governments. With heavy reliance on digital platforms for government services, financial transactions, communication and personal data storage, the risks associated with cyber threats have grown exponentially. Cyberattacks have surged in this decade with data breaches rising by 72% between 2021 and 2023, affecting over 343 million victims globally. The financial repercussions of these attacks are staggering, with the average data breach cost reaching $4.88 million in 2024.

Cybersecurity criminals target small local governments, K-12 schools and underserved communities because they lack the resources and capabilities to thwart these attacks.

These alarming statistics underscore the urgent need for robust cybersecurity measures to safeguard personal and organizational data. With the emergence of generative AI, cyberattacks are poised to become more complex and occur more frequently. State chief information security officers (CISOs) in the 2024 Deloitte-NASCIO Cybersecurity Study indicated they were only somewhat confident in their state’s ability to defend against AI-generated cyberattacks, creating a need to rapidly evolve existing whole-of-state defenses.

State CISOs are responsible for developing, implementing and enforcing security policies to protect critical data for all citizens. However, certain communities face disproportionate challenges in securing their digital environments. Underserved communities, including low-income families, rural communities, communities of color, military veterans, people with disabilities, tribal communities and immigrant populations are particularly vulnerable to cyber threats. These groups often lack the resources and support needed to defend against cyberattacks effectively. Cyber operations targeting these communities compromise their digital security and grow inequities associated with the digital divide. For example, the first-ever tribal-specific cybersecurity grant was passed this year, providing $18.2 million to Tribal Nations to improve their cybersecurity frameworks and reduce cyberattacks. While truly ground-breaking, this type of funding may run out quickly given the depth of cybersecurity challenges in tribal communities, future uncertainty surrounding budgets and partisan politics. The United States currently lacks a comprehensive response to address these uniquely targeted cybersecurity risks, placing more responsibility on state tech leaders to develop such protocol.

A case study conducted among low-income and non-English speaking residents of San Francisco provides an example of what many underserved communities across the nation experience regarding cybersecurity access. The study revealed several key findings, with surveyed residents indicating:

- **26%** **had been a victim of a cyber scam** (with 1/3 stating they had been scammed more than once)
- **40%** **had a personal device infected by a virus at least once**
- **17%** **willingly provided protected personal information to a stranger online**
- **39%** **do not create complex passwords**
- **49%** **do not check websites for security seals indicating legitimacy**

This study also compared cybersecurity awareness and knowledge with demographic information, revealing that those with higher income and educational attainment knew more about proper cybersecurity protocols than people with lower incomes and educational attainment.

Understanding Digital Exclusion

Many marginalized groups experience a variety of social, economic and physical factors that result in their exclusion from information technology, communication technology and digital services. This concept, known as digital exclusion, is characterized by three main factors: physical access, skills and inequalities of access. When framing digital exclusion through a cybersecurity lens:

1. **Physical access:** Marginalized groups without access to devices (including newer, updated models) and technology infrastructure are not able to use security technologies, increasing their risk of being compromised by cyberattacks.
2. **Skills:** Without access to digital literacy programs, such as online community training issued by governments or local libraries/government technology office branches, marginalized groups may be less likely to understand and properly use security and privacy features. This also increases the risk of being compromised.
3. **Inequalities of access:** While there are numerous factors that perpetuate inequalities of access to technology and cybersecurity measures, economic and design factors are two of the most pertinent. The cost of newer devices, travel time/cost from rural to metropolitan areas to use city services and inaccessible security features for older devices all contribute to increasing compromise risks for marginalized groups.

Barriers to Expanding Cybersecurity in Underserved Communities

State CISOs are aware of and trying to address cybersecurity needs in their state's underserved populations, however they encounter similar barriers

to expansion nationwide. One of the largest barriers is funding. Many state CISOs have expressed gratitude for State and Local Cybersecurity Grant Program (SLCGP) funding, however it may not be fully comprehensive. The 2024 Deloitte-NASCIO Cybersecurity Study revealed that only six CISOs felt they had all the grant funding they could use. While CISOs did indicate that their cybersecurity budgets are rising, funding is not increasing at the same rate as threats. Cybersecurity budgets must be funded enough to fully address the needs of all state residents, including those in underserved communities.

Receiving funding is one challenge, however fund dispersion is also a major hindrance CISOs are facing. Officials in local agencies may not be familiar enough with the funding application and procedures to successfully apply. Localities that do apply tend to be larger localities, with smaller ones not applying. No application from smaller underserved localities means no grant funding, increasing reliance on cheaper, less secure cybersecurity hardware.

Localities may also receive funding without direction, leading to hardware and software purchases that they cannot fully leverage. Implementing these new cybersecurity tools is further complicated by two main issues. First, officials in smaller, local agencies often lack cybersecurity training and awareness resulting in a lack of basic cyber hygiene. Second, cybersecurity infrastructure within local agencies may not be up to state standards and requirements.

Another challenge to cybersecurity expansion in underserved communities is population density. States with large rural areas and few metropolitan areas see a majority of the population

Another challenge to cybersecurity expansion in underserved communities is population density. States with large rural areas and few metropolitan areas see a majority of the population concentrated in major cities, making it difficult to keep momentum behind initiatives intended to benefit underserved communities.

concentrated in major cities, making it difficult to keep momentum behind initiatives intended to benefit underserved communities.

States are combatting these barriers in a variety of ways, including:

- Maximizing SLCGP funding by providing cash to localities that have thoroughly assessed needs in their communities and included detailed spending plans in proposals to address said needs.
- Issuing statewide toolkits for locality use.
- Pushing statewide initiatives, like intra-agency collaborative cybersecurity campaigns, that would especially benefit underserved communities and allow for bigger, up-to-standard communities to assist them; more examples of statewide initiatives are highlighted in the state spotlights at the end of this paper.
- Leveraging the state's buying power by adding cybersecurity services and tools to state master price contracts that underserved communities may use.
- Promoting the importance of cybersecurity as a vital, nonpartisan risk issue in state legislatures.
- Adopting .gov domains to provide secure and trusted domain addresses for all local government websites and applications.

Inclusive Security as the Way Forward

Combatting digital exclusion to protect everyone from cybersecurity threats will continue to grow in importance as threats rapidly evolve. However, this task can seem impossible given the nuances and complexity of improving cybersecurity in underserved communities. To best address this, states should shift towards an inclusive security approach – changing the mindset cybersecurity is approached with to promote change from the top down. Inclusive cybersecurity is a critical component of whole-of-state cybersecurity.

Inclusive security is an approach to cybersecurity and privacy that prioritizes making critical security technologies available to everyone despite their resources, ability and/or demographics.

It differs from the standard cybersecurity approach by equally prioritizing both threat exclusion/ prevention and enabling all people to live safer, more accessible digital lives. State technology leaders can begin to implement inclusive security measures by addressing the following steps:

1. **Intentionally develop and train cybersecurity officials in underserved communities.**
   As mentioned earlier, cybersecurity officials in underserved communities often lack the knowledge and resources needed to enhance cyber safety practices for their organizations and communities. Due to variations in resource allocation and distribution, states can prioritize enhancing the expertise of local officials by designing cybersecurity training tailored to each agency within a local government entity. Cybersecurity practices can differ based on an agency's specialization and the specific job descriptions of its employees, creating a need for more in-depth training aligned with these nuances. Additionally, states can develop specialized cybersecurity training for officials working in underserved communities. While these officials are typically aware of the unique challenges within their communities, they may be unsure how to address them. Providing targeted solutions and guidance through specialized training can boost local officials' confidence in their expertise, improving cybersecurity in underserved communities and fostering more trust between state and local officials.

2. **Ensure that digital government services include user-friendly, inclusive security features.** Marginalized groups can have less familiarity with security features for a variety of reasons, increasing their frustration when using necessary digital services. For example, an elderly citizen with nerve difficulties may not be able to accurately enter a numeric multi-factor authentication (MFA) code to access their benefits portal. Facial recognition or other biometric measures can be a more secure authentication method, but also more user-friendly for elderly users. Hiring an accessibility coordinator and incorporating human-centered design as a cybersecurity strategy can greatly improve accessibility expansion for all current and future state technology projects.

3. **Partner with nonprofits and other organizations that serve underserved communities in the state.** Improving cybersecurity accessibility and efficiency is a constantly evolving task, especially when it comes to underserved communities. Fortunately, nonprofit and other organizations provide services to and are housed within the target communities. By establishing a working partnership with these organizations, states can work to implement the following:
   - Conduct cybersecurity needs assessments to tailor assistance to specific needs.

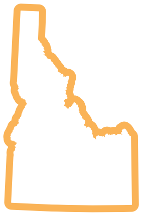
- Train nonprofit staff on cybersecurity awareness to equip them with the knowledge and tools necessary to help the underserved.
- Increase the reach of cybersecurity training and courses to marginalized communities.
- Hold town halls, open forums and participate in local events to increase cybersecurity awareness while gaining feedback / issue familiarization from the underserved.
- Engage members of marginalized communities in threat modeling, security design processes and technology demonstrations to receive important feedback from those most impacted by inaccessible security features.

4. **Partner with school technology personnel to provide early cybersecurity training to K-12 schools.** People of all ages can access the internet in a variety of ways. K-12 education heavily relies on technology to increase engagement and retention among students. Further, social media apps are heavily used by school-aged children – who also happen to be especially vulnerable to cybersecurity risks. Intervening early will help prevent children and their families from becoming victims of cyberattacks while instilling good digital hygiene at an early age. States should work with schools and school districts to hold cybersecurity training sessions in classrooms.

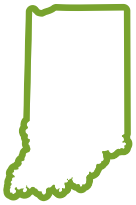
State Spotlights

Below are a few examples of how states are expanding cybersecurity in underserved communities. Many of these current practices are aligned with NASCIO's recommendations and have had success within the state.

NH: New Hampshire's Municipal Cyber Defense Program (MDCP) provides grant-funded cybersecurity training to municipal entities and residents through intra-agency partnerships between the Department of Information Technology, Department of Safety, NH Public Risk Management Exchange (PRIMEX) and the Atom Group. Through this collaborative effort, New Hampshire provides cybersecurity training to multiple groups, including residents, first responders, public-sector IT employees, educators, students, school boards, municipal leaders and elected officials. Training is tailored to specific group needs, including the type of agency/municipality, job descriptions and current levels of cybersecurity readiness in the agency/ municipality. By utilizing a "meet them where they are" approach to expanding cybersecurity, New Hampshire has fostered stronger relationships with local agencies and maximized the power of received funding to benefit all communities, including those underserved. In addition to MCDP, New Hampshire has also secured funding for ".GOV in a Box." This initiative provides funding for towns, cities, counties, police departments, fire departments, special districts and K-12 schools to transition to .gov domains to strengthen cybersecurity frameworks. Any agency or resident who would like to participate in these training courses simply fills out the application at https://www.theatomgroup.com/mcdp and search for ".GOV in a BOX" at https://www.doit.nh.gov/cybersecurity/state-and-local-cybersecurity-grant-program.



ID: The state of Idaho is expanding cybersecurity in rural underserved populations in various ways. Operation Cyber Idaho focuses on increasing cybersecurity competency, state and local collaboration and fostering trust by reinforcing localities with skilled cybersecurity professionals. These cybersecurity professionals come from those same rural Idaho communities, working in state apprenticeships and internships to gain the necessary skills before returning to their community to work full-time. This method builds trust and fosters collaboration between residents, localities and state technology leaders by developing "home-grown" talent that is familiar with Idaho's specific needs through their personal experience.



IN: The state of Indiana is addressing the expansion of cybersecurity in its rural underserved communities by building trust within localities. In addition to providing free online cybersecurity training, Indiana executed a campaign where state technology leaders visited localities to build rapport between state and local entities. Acknowledging that localities have strong relationships with each other, this campaign leveraged these existing relationships by using a word-of-mouth approach to expand cyber safety in rural communities. In turn, localities that have had success in reaching their cybersecurity goals by working with state technology leaders will share the outcomes with others, increasing their willingness to participate in more statewide cybersecurity efforts. This strategy may be especially useful in states where CISOs do not have statutory authority, but influence, over localities.

Conclusion

For states, prioritizing cybersecurity in underserved communities is not just a matter of protecting data but also of ensuring equal access for all citizens. Improving and expanding cybersecurity in underserved communities is a crucial element in whole-of-state cybersecurity practices. Addressing these unique challenges stemming from digital exclusion requires technological solutions and a commitment to incorporating diversity, equity, inclusion and accessibility practices into cybersecurity strategy. Adopting inclusive security practices can benefit underserved communities and entire populations, ensuring that all technology users are protected online. Understanding demographic trends in cyberattacks and fostering collaboration among cybersecurity professionals and underserved communities is the next step on the cybersecurity frontier.

Sources:

The Hidden Injustice of Cyberattacks

Cybersecurity Stats: Facts And Figures You Should Know

Improving Cybersecurity Awareness in Underserved Populations

Accessible and Inclusive Cyber Security: A Nuanced and Complex Challenge

DHS Announces $18.2 Million In First-Ever Tribal Cybersecurity Grant Program Awards

2024 Deloitte-NASCIO Cybersecurity Study

Michigan All In for the User: HCD - Our Strategy for Better Decisions

NASCIO Contact & Author

Kalea Young-Gibson, Policy Analyst
kyoung-gibson@NASCIO.org

Special thanks to state CISOs Ken Weeks (New Hampshire), Jerred Edgar (Idaho), and Hemant Jain (Indiana) for their contributions to this publication.

NASCIO Representing Chief Information Officers of the States

About NASCIO

Founded in 1969, the National Association of State Chief Information Officers (NASCIO) represents state chief information officers (CIOs) and information technology (IT) executives and managers from the states, territories and District of Columbia. NASCIO's mission is to foster government excellence through quality business practices, information management and technology policy. NASCIO provides state CIOs and state members with products and services designed to support the challenging role of the state CIO, stimulate the exchange of information and promote the adoption of IT best practices and innovations. From national conferences to peer networking, research and publications, briefings and government affairs, NASCIO is the premier network and resource for state CIOs.