Strengthening Cybersecurity in Rural Communities:

An Overview of Cost-Effective Strategies to Mitigate Threats

WRITTEN BY
Alexander Kinney, Ph.D

2026

INSTITUTE FOR HOMELAND SECURITY
SAM HOUSTON STATE UNIVERSITY

Strengthening Cybersecurity in Rural Communities:

An Overview of Cost-Effective Strategies to Mitigate Threats

Alexander Kinney

July, 2026

ABSTRACT

Rural communities face unique challenges in implementing effective cybersecurity measures due to limited access to resources. Limited funding, aging infrastructure, and shortages of trained IT professionals make it more difficult for organizations in these communities to implement best practices for mitigating cyber threats. Therefore, these organizations are disproportionately vulnerable to common cyberattacks. This paper examines cybersecurity preparedness challenges facing rural organizations operating in critical infrastructure sectors. I specifically evaluate approaches that align with the NIST Cybersecurity Framework (CSF) 2.0 and ISO/IEC 27001 information security standard, while remaining affordable and accessible to small-to-medium sized enterprises (SMEs). In doing so, I review the benefits and limitations of these strategies with the aim of identifying a realistic path forward for organizations in rural communities to enhance operational cybersecurity. The paper concludes with a discussion of practical recommendations for improving cybersecurity with special attention paid to how resilience matters for developing strategic partnerships with key stakeholders.

Contents

INTRODUCTION & OVERVIEW

The Growing Importance of Cybersecurity in Rural Communities

Cybersecurity readiness has become one of the central issues facing rural communities in today's digital landscape (Bholane, 2025). As digital technologies become increasingly integrated into everyday operations, many rural organizations continue to fall behind the curve in cybersecurity preparedness. Unique resource constraints that include financial limitations, outdated infrastructure, and the inability to recruit trained and experienced cybersecurity personnel, make cybersecurity more difficult (Grobler et al., 2011). Rapid technological advancement has also deepened the so-called "digital divide" between urban and rural communities (Lutzow, 2025). This has led to varying levels of cybersecurity awareness among those residing in rural communities that can have an outsized impact on organizations operating in these environments (Bholane, 2025).

These issues are especially significant in Texas, where rural organizations are the backbone of critical infrastructure sectors. Organizations operating in healthcare, energy production, chemical manufacturing, water and wastewater systems, and transportation networks have a substantial operational footprint in rural communities across the state. Though cyberattacks are more prevalent in urban areas due to a concentration of high value targets, rural organizations are arguably more vulnerable to threats (Alsmadi et al., 2023). The vast majority of rural organizations are "Small-to-Medium-Sized Enterprises" (SMEs) that frequently rely on digital technologies to support core functions required for daily operations (Wilmoth, 2023), and while these technologies have the capacity to make operations more efficient, they also increase exposure to a number of common cyberthreats (Chowdhury, 2016). Many of these threats are relatively inexpensive for attackers to execute, presenting a direct and immediate challenge to organizations that lack the appropriate safeguards (Goenka, Chawla, & Tiwari, 2024)

The growing scale and frequency of cyberattacks more broadly threatens to amplify these concerns in the coming decades. While the projected economic costs of cyberattacks are difficult to accurately ascertain, industry observers estimate that the annual global costs will range from hundreds of billions–to even several trillions–of dollars by the 2030s (Cobos & Cakir, 2024). In 2025, the total financial losses reported

to the FBI's Internet Crime Complaint Center (IC3) eclipsed the $20 billion mark for the first time (Federal Bureau of Investigation, 2025), and in Texas alone, 97,912 complaints were filed and losses surpassed $1.8 billion (Federal Bureau of Investigation, 2025). For many rural organizations, strategic, but modest, investments in cybersecurity preparedness today may substantially reduce the likelihood of disruption or financial losses that could otherwise threaten long-term organizational stability (Kesswani & Kumar, 2015), and potentially, national security (Etzioni, 2011).

Collectively, these factors create an environment where rural organizations are both more vulnerable to threats and less resilient when an attack occurs. For many rural organizations, the biggest challenge now transcends simply recognizing what a cyber threat looks like. It is instead to determine how to realistically build a portfolio of effective cybersecurity mitigation strategies that are cost-effective, scalable, and capable of reducing the growing preparedness gap between rural and urban organizations.

PROBLEM STATEMENT

Among the many threat mitigation strategies available to bolster cybersecurity, rural organizations are often forced to weigh operational effectiveness against financial feasibility. Many rural organizations operate below what industry observers refer to as the "cybersecurity poverty line," where advanced cybersecurity capabilities remain financially and operationally out of reach (Nather, 2024). Comprehensive approaches such as the NIST Cybersecurity Framework (CSF) 2.0 and ISO/IEC 27001 information security standard should still remain an aspirational goal for these organizations, but implementing these standards in full is often unrealistic for SMEs operating within resource-constrained environments. This preparedness deficit carries broader implications nationally and globally. Rural communities support many critical infrastructure sectors, including healthcare, agriculture and energy production, that play a vital role in promoting regional economic security and public safety. Despite the growing importance of cybersecurity preparedness in these sectors, SMEs struggle to identify meaningful opportunities to improve resilience in a financially sustainable way (Tetteh, 2024). This creates a need for more research to identify a path forward for these organizations (Chidukwani, Zander, and Koutsakis, 2022).

Research Objective

To identify a series of cost-effective strategies that can improve organizational resilience in rural communities, this paper evaluates findings from research on the cybersecurity needs of domestic and international SMEs operating within resource-constrained environments. First, it outlines common cybersecurity threats and vulnerabilities identified in this research. It then introduces the NIST Cybersecurity Framework (CSF) 2.0 and ISO/IEC 27001 information security standard and highlights best practices from these frameworks that organizations can reasonably implement while managing significant resource constraints. Finally, the paper explores how implementing these practices is increasingly becoming a prerequisite for establishing public-private partnerships that will be vital to rural organizational sustainability in the coming decades.

TOPIC DISCUSSION

Common Cyber Threats Facing Rural Critical Infrastructure

Rural organizations face exposure to many of the same cyber threats affecting their urban counterparts, but often without the equivalent defensive capabilities or institutional support (Alsmadi et al., 2023). Though a comprehensive overview of these threats is outside of the scope of this particular piece, the most common threats facing organizations include phishing attacks, ransomware, and distributed-denial-of-service (DDOS) attacks (Chapman, Leblanc, & Partington, 2011). These threats have become especially problematic in rural healthcare environments because successful attacks can be life-threatening (Lehmann & Kinney, 2023). These attacks remain common because they are inexpensive to execute while continuing to produce relatively high rates of success even against the most well-resourced organizations (Reed, 2024). As critical infrastructure organizations increasingly migrate their infrastructure online, the rapid development of generative AI has escalated concerns that relatively common cyberattacks will be even easier to carry out in the coming years (Gartner, 2024).

Cybersecurity Vulnerabilities Commonly Exhibited by Rural Organizations

The vast majority of organizations operating in rural environments are considered "small-to-medium size enterprises" (SMEs) (Wilmoth, 2023), because they employ fewer than 500 people (U.S. Small Business Administration, 2026). Recent reviews examining cybersecurity challenges facing SMEs have identified that there are recurring categories of preparedness challenges that SMEs commonly experience including limited cybersecurity literacy, a lack of economic resources, insufficient organizational alertness, and the absence of suitable cybersecurity guidelines that are tailored specifically to the SME business environment (Awan, Alam, & Kamran, 2025; Rombaldo, Becker, & Johnson, 2025). Collectively, this body of research provides a useful framework for understanding why cybersecurity preparedness remains difficult to achieve in many rural communities.

Knowledge and Literacy Challenges

Even though there is widespread belief among SMEs that they are knowledgeable about cybersecurity (Tetteh, 2024), research has shown that they often underestimate cybersecurity risks because employees and leadership teams lack a clear understanding of what constitutes a vulnerability to threat or even how a cyberattack occurs (Awan et al., 2025). SMEs also tend to lack awareness of existing vulnerabilities that have been identified by cybersecurity experts, or worse, come to view themselves as at a lesser risk of attack due to a misunderstanding of their own asset values (Romboldo et al., 2025). Consequently, many SMEs will not recognize how vulnerable their organization is to being compromised until after an incident occurs. This means that improving preparedness in rural organizations is just as much about building the capacity to take advantage of available cybersecurity training and educational opportunities as it is about raising awareness of cyber threats.

Economic and Resource Constraints

Though many SMEs recognize the importance of cybersecurity, limited financial flexibility represents one of the most frequently identified barriers to cybersecurity preparedness (Awan et al., 2025; Romboldo et al., 2025). With smaller budgets, SMEs are often caught in a careful balancing act of how to allocate resources between critical personnel needs and replacing aging infrastructure. This has led to persistent lags in technology uptake that further exacerbate deficits in cybersecurity preparedness (Osborn, 2015). Resource constraints extend beyond the ability to purchase new

technologies as well. SMEs frequently struggle to recruit and retain personnel with specialized cybersecurity expertise, forcing cybersecurity responsibilities onto employees already managing multiple operational duties (Bholane, 2025). These challenges explain why many rural organizations continue to operate below what has been described as the “cybersecurity poverty line” (Nather, 2024). Although many of these organizations are motivated to improve their cybersecurity preparedness, limited staffing capacity and competing operational priorities can make sustained investment difficult. As a result, improving preparedness in rural organizations means prioritizing strategies that provide meaningful improvements in resilience while minimizing costs.

Insufficient Organizational Alertness

Beyond awareness and resource limitations, many SMEs struggle to keep abreast of the evolving risks as digital technologies continue to develop at a rapid pace (Awan et al., 2025). New vulnerabilities and attack methods emerge faster than SMEs can reasonably evaluate them. At the same time, SMEs are confronted with a shifting regulatory environment that can make identifying meaningful information challenging (Patterson, 2026). These challenges are amplified in rural communities. With comparatively smaller staffing pools to their urban counterparts, rural organizations are more likely to focus on more immediate concerns like maintaining continuity of operations than long term planning for cybersecurity preparedness (Wasserman & Wasserman, 2022). Consequently, rural organizations will likely benefit from cybersecurity strategies that reduce the need for continuous monitoring and allow personnel to focus their attention where it is needed most (Chidukwani et al., 2022).

Lack of Tailored Guidance for SMEs

The stark reality is that existing guidelines and standards for cybersecurity preparedness are not specifically tailored to the types of operational conditions that are routinely navigated by SME’s (Awan et al., 2025). These standards were largely crafted with large enterprises at the forefront of concern which means that work still needs to be done to identify which recommendations SMEs should prioritize and how they should pursue meeting them (Ponsard & Grandclauden, 2019). In rural communities where specialized expertise may be limited, organizations may find themselves uncertain of where to begin. With this uncertainty in mind, rural organizations may be at an elevated risk of implementing cybersecurity solutions which cause more problems than they solve (Romboldo et al., 2025). This means that increasing preparedness among rural

organizations also requires moving beyond simply identifying what solutions are available to identifying which solutions can achieve the greatest fidelity to established cybersecurity standards while remaining tailored to their specific operational realities. It also means that rural organizations need structured prioritization methods that are capable of identifying where investments should be directed first.

Practical Cybersecurity Mitigation Strategies for Rural Organizations

While comprehensive implementation of cybersecurity standards may remain unrealistic for many rural organizations, established frameworks such as the NIST Cybersecurity Framework (CSF) 2.0 and ISO/IEC 27001 can still provide useful guidance regarding which practices are most effective at reducing organizational risk. Rather than treating them as rigid requirements, this paper looks to these standards as a source of specific practices that can provide meaningful improvements to cybersecurity preparedness. The following section highlights several strategies that align with established cybersecurity standards and may be implemented incrementally as organizations build cybersecurity capacity over time.

Conducting a Cybersecurity Risk Assessment & Framework Profile

Rural organizations rarely have the resources necessary to address every vulnerability simultaneously. Fortunately, both the NIST Cybersecurity Framework (CSF) 2.0 and ISO/IEC 27001 standard recognize that organizations must make decisions regarding which cybersecurity risks deserve immediate attention and which can be addressed over time (Nair & M.R., 2023). The first step for improving preparedness in any organization, rural or otherwise, should be a comprehensive cybersecurity risk assessment (Ansar et al., 2024). Conducting a risk assessment allows organizations to identify which assets are truly at risk and which systems are most vital to maintaining operations, and thus, in greatest need of protection.

For organizations operating in critical infrastructure sectors, risk assessments can be especially helpful, and importantly, affordable. Because many rural organizations lack the resources necessary to conduct extensive cybersecurity reviews internally, publicly available assessment tools can provide an accessible starting point for identifying vulnerabilities and prioritizing mitigation efforts. The Center for Cybersecurity & Infrastructure Security Agency (CISA) maintains a vetted bank of no-cost cybersecurity

risk assessment tools specifically available to organizations operating in critical infrastructure sectors. Other government agencies also offer specific tools tailored to critical infrastructure sectors. For instance, the Office of the National Coordinator for Health Information Technology offers the Security Risk Assessment Tool (SRA) specifically to U.S. healthcare providers.

Conducting a risk assessment helps rural organizations establish a clearer understanding of their “cyber-hygiene” (Ncubukezi, Mwanza, & Rocaries, 2020), while establishing a foundation for developing a CSF 2.0 Organizational Profile (National Institute of Standards and Technology, 2024a). A CSF 2.0 Organizational Profile is a customized roadmap for moving an organization from their current cybersecurity posture to desired, future cybersecurity stance. Rural organizations seeking additional guidance in this effort may also benefit from consulting the NIST Cybersecurity Framework 2.0 Small Business Quick-Start Guide which offers tailored guidance for SMEs with minimal or no cybersecurity plans in place to translate their risk assessments into actionable next steps (see National Institute of Standards and Technology, 2024b).

Prioritizing Cybersecurity Investments Using Criticality Assessments

With limited resources, rural organizations also continuously face the challenge of identifying where to focus investments on resilience. A traditional approach to manage this issue has been using a CARVER matrix to identify risk and rank threats (Young, 2025). Although originally developed for military target analysis, it can equip rural organizations with a useful method for deciding where to prioritize resources in a systematic fashion. Used alongside a CSF 2.0 Organizational Profile, a simplified CARVER-style assessment could help decision-makers figure out where systems are most vulnerable and most likely to produce cascading outcomes if compromised, though they should not be used in the place of a comprehensive risk assessment or sector-specific guidance. This tool evaluates organizational targets according to six factors: criticality, accessibility, recoverability, vulnerability, effect, and recognizability. Decision-makers rank each factor on a scale of 1-5. Finally, they sum the total across rows, producing a score for each to identify investment priorities. An example CARVER-style assessment is demonstrated below.

Figure 1. Example of Simplified CARVER Prioritization Matrix for Rural Organization

Asset/ System	Criticality	Access-ibility	Recover-ability	Vulner-ability	Recogniz-ability	Total Score
Water control system	3	4	1	2	5	15 (Intermediate Priority)
Customer Electronic records	5	5	2	1	3	16 (Intermediate Priority)
Billing/payroll system	5	1	5	4	4	19 (Highest Priority)
Public website	1	1	2	4	1	9 (Lowest Priority)

Note: This figure is an illustrative example only. Organizations should assign scores based on their own operational environment.

Strategic Cybersecurity Education and Training Initiatives

The NIST Cybersecurity Framework (CSF) 2.0 and ISO/IEC 27001 standard place emphasis on the importance of ensuring that employees understand the crucial role that they play in cybersecurity (Nair & M.R., 2023). The reality is that many cyberattacks succeed because employees unknowingly grant access to organizational systems through phishing schemes, weak passwords, or other forms of social engineering (Tetteh, 2024). Though it can be challenging for rural organizations to divert resources toward cybersecurity training and education initiatives, improving employee awareness remains one of the best methods available for reducing exposure to common cyber threats.

The pressing issue facing rural organizations is how to identify training programs that are reputable, accessible, and most importantly, effective (Abrahams et al., 2024). A good starting point is to look toward official options as these are both vetted and affordable. For instance, the National Initiative for Cybersecurity Careers and Studies (NICCS), sponsored by CISA, offers no-cost online cybersecurity training to government

employees, contractors, and U.S. residents through its Learning Management System (LMS). The Federal Emergency Management Agency (FEMA) also sponsors no-cost cybersecurity training options through strategic partnerships with flagship colleges and universities. Currently, Texas residents can take advantage of this opportunity through Texas A&M's Engineering Extension Service. Both of these options have the advantage of being self-paced, allowing organizations to improve cybersecurity literacy by fitting into an already resource constrained operational workflow.

Best practices dictate that organizations should consider incorporating cybersecurity awareness training as a routine professional development activity rather than a one-time requirement (Ansar et al., 2024). Self-paced training options sponsored by trusted public institutions can help organizations improve cybersecurity literacy without requiring substantial investments of time or money. As this illustrates, addressing the knowledge and literacy challenges discussed previously does not necessarily require significant financial investment, but rather a commitment to making cybersecurity education a routine component of organizational operations.

Layering Security Controls

No cybersecurity control can protect an organization from every threat. This is why the NIST Cybersecurity Framework (CSF) 2.0 and ISO/IEC 27001 emphasize the importance of implementing multiple complimentary controls to help organizations address risk (Nair & M.R., 2023; Ansar et al., 2024). The NIST Cybersecurity Framework (CSF) 2.0 aligns activities across six dimensions: 1. Govern, 2. Identify, 3. Protect, 4. Detect, 5. Respond, and 6. Recover. Together, these dimensions provide a structured framework for how to select complementary security controls that produce a layered approach to risk mitigation (Tetteh, 2024).

Some of the most effective controls are among the most affordable options. The NIST CSF 2.0 Small Business Quick-Start Guide specifically highlights the importance of multi-factor authentication (MFA) tools, password managers, proactive software updates, and regular data backups as industry standard practices that can reduce exposure to common cyberthreats. Other controls, like application firewalls and enterprise-level antivirus software, have been identified as important, cost-effective solutions for cybersecurity preparedness (Ansar et al., 2024). Many of these controls are already implemented in popular commercial operating systems and cloud platforms.

Additional cybersecurity tools endorsed by CISA may also be available at little or no cost through publicly available resource directories and sponsored listings (see CISA, 2026).

The effectiveness of layered security controls stems from the fact that this approach minimizes vulnerabilities across operational domains (Aggarwal, Saxena, & Sharma, 2025). MFA tools and password managers can help reduce likelihood of unauthorized access. Automatic software updates reduce exposure to known vulnerabilities before organizational personnel become aware of potential exploits. Firewalls and antivirus software offer real-time threat identification as a form of pro-active risk management (Gangieni et al., 2021). In this sense, a layered approach helps rural organizations incrementally build capabilities across the six dimensions of the NIST Cybersecurity Framework (CSF) 2.0 outlined above.

Incident Response and Recovery Planning

Cybersecurity experts have been clear that the overarching goal of a cybersecurity program is to carefully evaluate what level of risk is tolerable to organizational operations and prepare accordingly, not to try to eliminate risk entirely (Nair & M.R., 2023). Even organizations with robust cybersecurity controls remain vulnerable to cyberattacks. This makes incident response and recovery planning essential components of cybersecurity preparedness and helps to align organizations with the NIST Cybersecurity Framework (CSF) 2.0 and ISO/IEC 27001, both of which emphasize the importance of having a formal set of procedures for addressing cybersecurity incidents.

The biggest question facing rural organizations that may not yet have such a plan is how to go about crafting one given the significant resource constraints that they are operating under (Bholane, 2025). One of the most common misconceptions regarding incident response is believing that simply having a written response plan is sufficient enough (Thompson, 2018). Instead, effective incident response planning should be viewed as an ongoing organizational program. Many organizations struggle during cybersecurity incidents because they have failed to adequately determine who is responsible for making decisions, how incidents should be escalated, and what procedures should be followed when disruptions occur (Thompson, 2018).

The NIST CSF 2.0 Small Business Quick-Start Guide recommends that a basic incident response plan should include the following things: 1. Who is responsible for coordinating response efforts, 2. How incidents should be reported, and 3. What escalation procedures should be followed when an incident occurs (National Institute of Standards and Technology, 2024b). Organizations should periodically rehearse these procedures to ensure that personnel understand their responsibilities prior to an incident. Thompson (2018) recommends that this preparation helps to reduce confusion so that response teams can coordinate more effectively.

Recovery planning is just as important as response planning as well. Both NIST CSF 2.0 and ISO/IEC 27001 emphasize that organizations should maintain reliable data backups, keep written documentation establishing recovery procedures, and periodically test these processes to ensure that critical systems can safely be returned to operation following a disruption (National Institute of Standards and Technology, 2024; Nair & M.R., 2023). These are core components to an effective incident response plan because organizations will ultimately be judged on their ability to restore operations following a disruption (Thompson, 2018).

Incident response and recovery planning is not entirely cost-free, particularly because it requires organizations to devote one of their most precious resources–time. However, this investment could be considered modest when compared to the costs associated with an ineffective response to a cybersecurity incident (Kesswani & Kumar, 2015). In this sense, a comprehensive incident response plan represents one of the most cost-effective investments available to rural organizations because it improves resilience without requiring substantial financial expenditures on new technologies.

WAY FORWARD

The discussion thus far has centered on practical strategies that rural organizations can implement to improve cybersecurity preparedness from the vantage point that resilience has self-evident benefits for mitigating cyberattacks. Beyond reducing risk and improving resilience, cybersecurity preparedness is increasingly becoming a factor influencing how organizations are evaluated by key external stakeholders. These evaluations can have downstream impacts on economic opportunities (Carr, 2016). As cybersecurity threats have become more prominent, new certifications and accreditation standards have emerged as a prerequisite for securing collaborative opportunities (Chaney, 2025). In other words, effective cybersecurity is quickly becoming a necessary element of partnerships that many critical infrastructure organizations located in rural communities currently depend on or will come to depend on in the near future. In this section, the paper explores how cybersecurity preparedness matters for market access and for building public-private partnerships.

Cybersecurity Preparedness as Market Access

One of the clearest examples of the growing relationship between cybersecurity preparedness and organizational opportunity can be found in the Cybersecurity Maturity Model Certification (CMMC) (see Department of Defense, 2026). Under CMMC, organizations seeking to participate in certain defense contracting opportunities must demonstrate that they maintain cybersecurity practices consistent with established security standards. CMMC is particularly noteworthy because it reflects a broader shift occurring across both public and private sectors (Chaney, 2025).

This trend is not limited to defense contracting either. Organizations that operate in other critical infrastructure sectors are increasingly encountering new cybersecurity preparedness expectations tied to accreditation standards that increasingly influence partnership agreements. For instance, organizations that want to partner with providers supporting the bulk power system may encounter requirements that are influenced by an evolving list of reliability standards put forth by the North American Electric Reliability Corporation (see NERC, 2026). Energy companies have long been evaluated under the Cybersecurity Capability Maturity Model (C2M2) sponsored by the U.S. Department of

Energy (see U.S. Department of Energy, 2026). Likewise, businesses partnering with healthcare organizations are expected to align their cybersecurity practices with the HITRUST security standards (see HITRUST, 2025).

Collectively, these examples illustrate a broader trend. Cybersecurity preparedness has now become a signal of organizational credibility and measure of suitability for participating in critical infrastructure markets. For rural organizations, the implications of this shift are significant. Industry observers also project that standards such as the CMMC will “flow down” into state and local government cybersecurity requirements for vendor contracting (Lohrmann, 2025). Moreover, cybersecurity mitigation strategies are now being viewed as signals of organizational credibility and can create a competitive advantage for businesses (Mmango & Gundu, 2024). Organizations that can proactively demonstrate alignment with notable cybersecurity standards are better positioned to secure contracts and access resources in an already resource constrained environment.

Building Capacity Through Public-Private Partnerships

Another challenge facing many rural organizations in overcoming the preparedness gap is simply generating the capacity to build resilience. Throughout this paper, personnel issues and fiscal constraints have consistently emerged as a significant barrier to identifying and implementing risk mitigation efforts. Thus, improving cybersecurity preparedness starts with implementing the affordable strategies outlined above to align organizational operations with industry standards. It moves forward by finding new opportunities to build capacity for further resilience efforts through cooperative efforts between public agencies, private organizations, and community stakeholders.

A promising avenue for rural organizations to pursue these collaborative opportunities can be found in Information Sharing and Analysis Centers (ISACs). ISACs serve as multilateral information sharing clearinghouses for critical infrastructure organizations operating in the private and public sector on all matters related to cybersecurity and threats (Powner, 2005). They also facilitate collaborative, cross-sectoral partnership opportunities. There is critical infrastructure specific ISACs like the Health-ISAC for healthcare organizations, the E-ISAC and ONE-ISAC organizations in the energy sector, and WaterISAC for organizations in the water sector. There are also information-technology specific ISACs that offer member organizations cybersecurity consulting

services like IT-ISAC and CyberShare–the latter of which is an extension of The Rural Broadband Association (see National Council of ISACS, 2026).

For rural organizations, the value of these partnerships extends beyond the cybersecurity resources they provide. Though some ISACs charge a nominal fee for membership, these fees are typically scaled to accommodate organizational size to allow SMEs access. Public organizations in Texas also now have access to the Multi-State Information Sharing and Analysis Center (MS-ISAC) free of charge (see Texas Department of Information Resources, 2026). By helping to distribute expertise across networks of organizations, ISACs reduce the need for every organization to independently monitor emerging threats and promote collective mitigation strategies. In doing so, they create opportunities for smaller organizations to benefit from collective situational awareness and shared cybersecurity expertise that might otherwise remain concentrated within larger institutions. In this sense, strategic public-private partnerships provide one of the most realistic avenues for rural organizations to narrow the cybersecurity preparedness gap in an affordable way.

CONCLUSION

While the growing integration of digital technologies across critical infrastructure sectors has created new opportunities for rural organizations, it has also exposed them to an expanding array of cybersecurity threats. This paper demonstrates that although rural organizations often operate under significant resource constraints, meaningful improvements in cybersecurity preparedness are not out of reach. It highlights several cost-effective strategies aligned with the NIST Cybersecurity Framework (CSF) 2.0 and ISO/IEC 27001 information security standard, including risk assessments, structured criticality assessments, workforce training initiatives, layered security controls, and incident response planning that offer practical starting points for organizations seeking to improve preparedness while operating within significant financial and personnel constraints. This paper also illustrates the growing importance of accreditation standards and partnership requirements, suggesting that preparedness is becoming an increasingly important factor in determining access to markets that are crucial for rural organizational sustainability. Finally, this paper argues that narrowing the cybersecurity

preparedness gap between rural and urban organizations will require sustained efforts to build capacity through strategic public-private partnerships, and particular, engagement with ISACs to expand access to cybersecurity expertise and resources. By pursuing these efforts, rural communities will be better positioned to strengthen regional and national critical infrastructure systems.

REFERENCES

Abrahams, T. O., Farayola, O. A., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Cybersecurity awareness and education programs: A review of employee engagement and accountability. *Computer Science & IT Research Journal*, *5*(1), 100–119.

Aggarwal, D., Saxena, A. B., & Sharma, D. (2025). Mitigating Cybersecurity Risks in IoT: A Layered Approach to Threat Detection and Prevention. *2025 4th International Conference on Sentiment Analysis and Deep Learning (ICSADL)*, 501–505. https://doi.org/10.1109/ICSADL65848.2025.10933329

Alsmadi, I., Tsado, L., & Gibson, C. (2023). Towards Cyber Readiness Assessment in Rural Areas. In K. Daimi & A. Al Sadoon (Eds.), *Proceedings of the 2023 International Conference on Advances in Computing Research (ACR'23)* (pp. 630–639). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-33743-7_50

Ansar, N., Parveen, S., Alankar, B., & Khan, I. R. (2024). Cost-Effective Cybersecurity Framework for Small and Medium-Sized Enterprises. In V. Goar, A. Sharma, J. Shin, & M. F. Mridha (Eds.), *Deep Learning and Visual Artificial Intelligence* (pp. 133–155). Springer Nature Singapore. https://doi.org/10.1007/978-981-97-4533-3_11

Awan, M., Alam, A., & Kamran, M. (2025). Cybersecurity Challenges in Small and Medium Enterprises: A Scoping Review. *Journal of Cyber Security and Risk*, *2025*(3), 89–102. https://doi.org/10.63180/jcsra.thestap.2025.3.7

Bholane, D. K. (2025). *BRIDGING THE DIGITAL DIVIDE: UNDERSTANDING CONSUMER AWARENESS TOWARDS CYBER SECURITY IN RURAL AND URBAN COMMUNITIES* (SSRN Scholarly Paper No. 5100525). Social Science Research Network. https://doi.org/10.2139/ssrn.5100525

CARR, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43–62. https://doi.org/10.1111/1468-2346.12504

Chaney, P. (2025). *The Business Impact of CMMC 2.0: What C-Suite and IT Leaders Must Know Now* (SSRN Scholarly Paper No. 5676342). Social Science Research Network. https://doi.org/10.2139/ssrn.5676342

Chapman, I. M., Leblanc, S. P., & Partington, A. (2011). Taxonomy of cyber attacks and simulation of their effects. *Proceedings of the 2011 Military Modeling & Simulation Symposium*, 73–80. https://dl.acm.org/doi/abs/10.5555/2048558.2048569

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. *IEEE Access*, *10*, 85701–85719. https://doi.org/10.1109/ACCESS.2022.3197899

Chowdhury, A. (2016). Recent Cyber Security Attacks and Their Mitigation Approaches – An Overview. *Applications and Techniques for Cybersecurity*. 6th International Conference, ATIS 2016 Cairns, QLD, Australia, October 26–28, 2016 Proceedings.

CISA. (2026). *No-Cost Cybersecurity Services and Tools*. https://www.cisa.gov/resources-tools/resources/no-cost-cybersecurity-services-and-tools

Cobos, E. V., & Cakir, S. (2024). A review of the economic costs of cyber incidents. *World Bank, Washington, DC, USA, Rep*, *193919*. https://documents1.worldbank.org/curated/en/099092324164536687/pdf/p17876919ffee4079180e81701969ad0a18.pdf

Department of Defense. (2026). *CIO - About CMMC*. https://dodcio.defense.gov/cmmc/About/

Etzioni, A. (2011). Cybersecurity in the Private Sector. *Issues in Science and Technology*, *28*(1), 58–62.

Federal Bureau of Investigation. (2025). *2025 IC3 Annual Report*. https://www.ic3.gov/annualreport/reports

Gangineni, V. N., Pabbineedi, S., Penmetsa, M., Bhumireddy, J. R., Chalasani, R., & Tyagadurgam, M. S. V. (2021). *Strengthening Cybersecurity Governance: The Impact of Firewalls on Risk Management* (SSRN Scholarly Paper No. 5451615). Social Science Research Network. https://papers.ssrn.com/abstract=5451615

Gartner. (2024, August 28). *Gartner Forecasts Global Information Security Spending to Grow 15% in 2025*. https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025

Goenka, R., Chawla, M., & Tiwari, N. (2024). A comprehensive survey of phishing: Mediums, intended targets, attack and defence techniques and a novel taxonomy. *International Journal of Information Security*, *23*(2), 819–848.

Grobler, M., Dlamini, Z., Ngobeni, S., & Labuschagne, A. (2011). Towards a Cyber security aware rural community. *ISSA*. https://www.researchgate.net/profile/Marthie-Grobler-2/publication/220803166_Towards_a_Cyber_security_aware_rural_community/links/53e8f1ce0cf28f342f3e5483/Towards-a-Cyber-security-aware-rural-community.pdf

HITRUST. (2025). *HITRUST CSF PDF* (11.8.0). HITRUST. https://hitrustalliance.net/

Junior, C. R., Becker, I., & Johnson, S. (2025). *Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity* (arXiv:2309.17186). arXiv. https://doi.org/10.48550/arXiv.2309.17186

Kesswani, N., & Kumar, S. (2015). Maintaining Cyber Security: Implications, Cost and Returns. *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*, 161–164. https://doi.org/10.1145/2751957.2751976

Lehmann, P. S., & Kinney, A. B. (2023). *Mitigating Cybersecurity Threats to Hospitals and Healthcare Facilities*. https://shsu-ir.tdl.org/items/d07971a3-5b85-4322-8c10-5c5d9feaf432

Lohrmann, D. (2025, October 5). *CMMC Is Finalized. How Will It Impact State and Local Government?* GovTech. https://www.govtech.com/blogs/lohrmann-on-cybersecurity/cmmc-is-finalized-how-will-it-impact-state-and-local-government

Lutzow, C. R. (2025). *Rural America's Digital Divide and Hybridized Internet Access* (SSRN Scholarly Paper No. 5913164). Social Science Research Network. https://doi.org/10.2139/ssrn.5913164

Mmango, N., & Gundu, T. (2024). Cybersecurity as a Competitive Advantage for Entrepreneurs. In A. Gerber (Ed.), *South African Computer Science and Information Systems Research Trends* (pp. 374–387). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-64881-6_22

Nair, A., & M.R., G. M. (2023). Mastering Information Security Compliance Management: A comprehensive handbook on ISO/IEC 27001:2022 compliance. Packt Publishing.

Nather. W (2024, October 8). *CTA Webinar*. https://www.youtube.com/watch?v=P8RP4QcygzY

National Council of ISACS. (2026). *Member ISACS*. https://www.nationalisacs.org/members

National Institute of Standards and Technology. (2024a, February). *NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide*. https://doi.org/10.6028/NIST.SP.1300

National Institute of Standards and Technology. (2024b, February 26). *The NIST Cybersecurity Framework (CSF) 2.0*. U.S. Department of Commerce.

Ncubukezi, T., Mwansa, L., & Rocaries, F. (2020). A review of the current cyber hygiene in small and medium-sized businesses. *2020 15th International Conference for Internet Technology and Secured Transactions (ICITST)*, 1–6. https://ieeexplore.ieee.org/abstract/document/9351339/

North American Electric Reliability Corp. (2026). *NERC CIP*. https://www.nerc.com/standards/reliability-standards/cip

Osborn, E. (2015). *Business versus technology: Sources of the perceived lack of cyber security in SMEs*. https://ora.ox.ac.uk/objects/uuid:4363144b-5667-4fdd-8cd3-b8e35436107e

Patterson, E. (2026). Cybersecurity Disparities in U.S. Healthcare: Regulatory Gaps, Equity Failures, and Systemic Risks. *DePaul Journal of Health Care Law*, *27*(1). https://via.library.depaul.edu/jhcl/vol27/iss1/4

Ponsard, C., & Grandclaudon, J. (2019). Survey and Guidelines for the Design and Deployment of a Cyber Security Label for SMEs. In P. Mori, S. Furnell, & O. Camp (Eds.), *Information Systems Security and Privacy* (Vol. 977, pp. 240–260). Springer International Publishing. https://doi.org/10.1007/978-3-030-25109-3_13

Powner, D. A. (2005). Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities. DIANE Publishing.

Reed, J. (2024, November 15). *Cybersecurity dominates concerns among the C-suite, small businesses and the nation | IBM*. https://www.ibm.com/think/insights/cybersecurity-dominates-concerns-c-suite-small-businesses-nation

Tetteh, A. K. (2024). Cybersecurity needs for SMEs. *Issues in Information Systems*, *25*(1). https://iacis.org/iis/2024/1_iis_2024_235-246.pdf

Texas Department of Information Resources. (2026). *Texas Secures MS-ISAC Statewide Membership on Behalf of Texas Government Entities | Texas Department of Information Resources*. https://dir.texas.gov/news/texas-secures-ms-isac-statewide-membership-behalf-texas-government-entities

Thompson, E. C. (2018). *Cybersecurity incident response: How to contain, eradicate, and recover from incidents*. Apress. https://books.google.com/books?hl=en&lr=&id=DXhvDwAAQBAJ&oi=fnd&pg=PR3&dq=thompson+cybersecurity+incident+response&ots=-Y4dhF1Ej4&sig=L1F68WhiPRV7zDP3y2YJ2roxwno

U.S. Department of Energy. (2026). *C2M2*. https://c2m2.doe.gov/

U.S. Small Business Administration. (2026). *Basic requirements | U.S. Small Business Administration*. https://www.sba.gov/federal-contracting/contracting-guide/basic-requirements

Wasserman, L., & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). *Frontiers in Digital Health*, *4*. https://doi.org/10.3389/fdgth.2022.862221

Wilmoth, D. (2023, August 22). *Small Business Facts: Small Businesses in Rural Areas*. U.S. Small Business Administration. https://advocacy.sba.gov/2023/08/22/small-businesses-in-rural-areas/

Young, D. (2025, May 13). *What is CARVER and When Should You Use it?* Circadian Risk. https://www.circadianrisk.com/resources/blog/what-is-carver-and-when-should-you-use-it

Author Biography

Alexander B. Kinney, Ph.D., is an Assistant Professor in the Department of Sociology at Oberlin College. His research unpacks the dynamics of social control in gray markets, uses automated text modeling algorithms to study the logics of deviant behavior, and theorizes punishment in a cross-historical context. Recently, his work has been published in Social Problems, Crime & Delinquency, and Law & Policy, among other journals.

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Water/Wastewater, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security

Sam Houston State University

Kinney, A. (2026). Strengthening Cybersecurity in Rural Communities: An Overview of Cost-Effective Strategies to Mitigate Threats. (Report No. 2026-1051). The Sam Houston State University Institute for Homeland Security. https://doi.org/10.17605/OSF.IO/9ZK28

INSTITUTE FOR HOMELAND SECURITY
SAM HOUSTON STATE UNIVERSITY