THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 2, 201-223
https://doi.org/10.55682/cdr/ys0t-9tc9

PROFESSIONAL COMMENTARY

Strengthening Cyber Resilience by Building Critical Infrastructure Communities: the C-CIC Pilot Study

Anne M. Chance*[1], Volker Franke[12], Timo A. Zwarg[2]

[1]TRENDS Global, Marietta, GA, USA
[2]Kennesaw State University, Kennesaw, GA, USA

Community resilience is crucial in addressing cyber threats to critical infrastructure, as these threats are often complex and require a multi-layered approach. In this paper, we explore how practices used to build trust and mutual support in face-to-face communities can be adapted to strengthen cyber resilience. Specifically, we apply the idea of community resilience as an effective response to cyber threats by examining the importance of building trust and social capital and discussing lessons learned from a pilot project designed to establish an intentional online cyber critical infrastructure community (C-CIC) in the metro Atlanta area. By analyzing the interplay of technological affordances, social norms, and individual behaviors, this research offers a deeper understanding of how trust shapes the structure and function of resilient cyber community ecosystems. Based on lessons learned from the Atlanta C-CIC pilot, the paper concludes with recommendations for building effective intentional online cyber critical infrastructure communities.

Keywords: cybersecurity, critical infrastructure, community-building, resilience, trust, online community, social capital

* Corresponding author: anne@trendsglobal.org

1 INTRODUCTION

> Our nation's critical infrastructure—the services Americans rely on every day—is under continuous threat by nation-state cyber adversaries and cybercriminal organizations around the globe. Over the last several years, we've witnessed increasingly frequent and complex attacks against small and medium-sized businesses, K-12 schools, water utilities, and healthcare organizations, including hospitals, which were in the past considered "off-limits." - Nitin Natarajan, Deputy Director Cybersecurity and Infrastructure Security Agency (CISA), January 7, 2025

Critical infrastructure provides services essential for the functioning of a productive modern society; it encompasses utilities, finance, healthcare, telecommunication, and emergency services, among others. In recent years, critical infrastructure has increasingly been the target of cyberattacks around the globe. In the spring of 2018, cybercriminals launched a ransomware attack against the city of Atlanta that restricted access to a wide range of online platforms, municipal operations, and databases. Although the city did not pay the ransom, the attack resulted in millions of dollars in damage, and it took several months for services to be fully restored (Young 2021). Beginning in 2019, the Russian Foreign Intelligence Service (SVR) attacked the computing networks of the Texas-based SolarWinds network management software company. SVR inserted malicious code into a routine software update, which allowed them to gain widespread access to government agencies and Fortune 500 companies (Government Accountability Office 2021). In May 2021, hackers disrupted operations of the Colonial Pipeline, causing fuel shortages and panic buying across the Eastern Seaboard (Wood 2023). These examples illustrate the different ways threat actors exploit the vulnerabilities of both public and private sector critical infrastructure organizations.

To test and improve critical infrastructure resilience against cyberattacks, the Army Cyber Institute (ACI) developed *Jack Voltaic*, a cyber research project and exercise series. *Jack Voltaic* brings together military and civilian partners, including local/city governments and private companies. Since 2016, ACI and partners have iteratively designed and conducted these exercises to stress-test collective responses to cascading cyber incidents. The exercises repeatedly revealed the same critical gap: technical systems often fail because the humans responsible for protecting them lack the social infrastructure necessary for coordinated response at scale (ACI 2021a, 2018, 2021b, 2022). As the *Jack Voltaic 3.0 Research Report* bluntly states, "crisis management and remediation is personality driven" and municipalities "tend to lack experience with real cyber events and thus have difficulty visualizing second-, third-, and fourth-order effects." The exercises have consistently shown that cyber resilience depends on personal relationships and the need for institutionalization (ACI 2021a).

We developed the *Critical Sherpas* pilot in metro Atlanta to test a core hypothesis derived from the *Jack Voltaic* exercises: that establishing pre-incident social networks is essential for effective cyber defense. This intentional online community serves as a laboratory for

adapting face-to-face trust-building to a digital environment. The moniker *Critical Sherpas* reflects the community's vital role as expert guides who navigate the treacherous terrain of modern cyber threats on behalf of the public.

Community psychology and sociological research demonstrate that key factors strengthening resilience in physical communities are trust, social capital, and mutual aid networks (Norris et al. 2008; Tierney 2019). Starting with the assumption that the same principles apply to cyber defense (Castelfranchi, Falcone, and Marzo 2006), this paper explores how practices used to build trust and mutual support in face-to-face communities can be adapted to digital and online communities to strengthen cyber resilience. Drawing on observations from the *Critical Sherpas* pilot and beta test, we examine how an intentionally designed online cyber critical infrastructure community (C-CIC) can strengthen cyber resilience by improving cross-sector coordination, information sharing, and collective cyber defense capabilities.

Drawing on Metcalf (2004), Bohill (2010) defines an *intentional community* as a voluntary assembly of individuals from diverse backgrounds who convene to address perceived social inadequacies. These groups foster a distinct "we-consciousness" by adopting shared practices and a consciously devised culture that serves as an alternative to mainstream society. Accordingly, we define the C-CIC as an intentionally designed network of individuals from diverse professional backgrounds, who voluntarily convene online to address shared vulnerabilities and systemic challenges within cyber and critical infrastructure domains.

We first examine the theoretical importance of trust and social capital in physical and virtual communities from the literature. After introducing the key factors and considerations guiding the design of the *Critical Sherpas* C-CIC pilot, we discuss insights derived from beta testing feedback. The purpose of our research is to inform collaborative efforts between cyber professionals, critical infrastructure operators, government, and private sector leaders seeking to intentionally design C-CICs to improve cyber resilience of critical infrastructure.

2 BACKGROUND AND LITERATURE REVIEW

2.1 Cyber Resilience of Critical Infrastructure

The National Institute of Standards and Technology (NIST) defines cyber resilience as "The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment" (NIST, 2024, 2022, 2021).

We define community resilience as a community's capacity to anticipate, absorb, adapt to, and transform through disruption, whether social, economic, environmental, or political. Rather than simply bouncing back to a previous state, we see resilience as an emergent strength, a process in which communities become more equitable, inclusive, and cohesive

by navigating challenges together. This perspective is informed by established research approaches focusing on structural violence (Chance 2023; Galtung 1990; Galtung and Höivik 1971; Galtung 1969), trauma-informed practices (Erickson and Harvey 2023), and conflict transformation (Lederach 2005). This definition reinforces the importance of social capital, trauma awareness, and participatory processes that help empower historically underserved voices. In the C-CIC pilot, our objective was to improve community resilience by creating online spaces where collaboration could thrive.

Whereas cybersecurity focuses on protecting digital assets and preventing breaches, cyber resilience presumes that intrusions will occur. It emphasizes both functional continuity and system adaptation despite reduced capability (Linkov and Kott 2018). Smith (2023) argues that cyber resilience depends on system properties such as critical thresholds, recovery times, and adaptive learning. Björck et al. (2015) also focuses on operational continuity and highlights the importance of strategic planning to achieve intended outcomes. This is particularly important (and therefore challenging) because cyber resilience is a dynamic, system-wide capability that spans technical, human, and institutional domains.

Municipalities and smaller organizations are especially vulnerable to cyber threats due to limited budgets, underinvestment, inconsistent governance, outdated IT systems, and insufficient staff training. This also makes them attractive targets for ransomware. Additionally, small businesses often face risks through third-party services and supply chain compromises (Hossain et al. 2024). The consequences are real and can be severe. As the 2023 Hiscox Cyber Readiness Report shows, in 2022, 41 percent of small businesses were targets of cyberattacks, and spent an average of $16,000 in ransom. Only half recovered all their data, while the other half had to rebuild their systems (Hiscox 2023). In 2021, 61 percent of small businesses were targeted, and their employees experienced over three times as many social engineering attacks as those at larger enterprises (Rahmonbek 2025).

Mitigating these threats requires human-centered, collaborative solutions. Strategic alliances between local governments, businesses, academic institutions, and other municipalities have been shown to improve collective response by enabling the sharing of threat intelligence, best practices, and pooled resources (Hossain et al. 2024). Social connections and collective support play a critical role in helping individuals and groups withstand and recover from adversity and disruption. When people are connected to and supported by others, their ability to bounce back from challenges is significantly strengthened (Tierney 2019).

Cyber resilience is stronger when those responsible for protecting critical infrastructure know each other personally, understand local vulnerabilities and interdependencies, and can coordinate rapidly during crises. In face-to-face communities, such relationships traditionally developed organically through professional associations, shared workplaces, or community organizations. However, the realities of modern cybersecurity work make regular in-person coordination between disparate professions, areas of expertise, and jurisdictional purviews

challenging. This creates a compelling case for connecting local cyber professionals through online platforms. While hybrid approaches that also incorporate face-to-face relationship-building might be optimal, practical constraints often necessitate virtual connectivity.

To enable effective collective action, online cybersecurity communities must be intentionally designed to foster trust and social capital.

2.2 Trust

Trust is a cornerstone of cyber resilience for interdependent critical infrastructure sectors (e.g., energy, water, transportation) where a disruption in one sector can cause cascading failures. Defending essential services requires effective collaboration among diverse stakeholders from government agencies, private industry, and emergency response teams. In such communities, trust is deeply embedded in social relationships, peer interactions, and shared norms (Wu, Edwards, and Das 2022).

A collaborative online platform for stakeholders can enhance preparedness and response, but its effectiveness ultimately hinges on cultivating trust among users. This is essential because key security behaviors, like information sharing and crisis coordination, are fundamentally social processes (Wu, Edwards, and Das 2022). As is the case with consumer products and brands (Harrigan et al. 2021), community members must trust the beliefs and intentions of both their peers and the platform itself. A lack of trust in digital spaces may lead to siloed information sharing, misinformation, and hesitancy in adopting collaborative security measures (Collett 2021). Without trusted networks, stakeholders may withhold threat intelligence out of fear of reputational damage or competitive disadvantage. This can lead to fragmented crisis response, exacerbate vulnerabilities, prolong recovery, and erode public confidence in leaders' ability to protect essential services (Backman 2021).

2.3 Social Capital

Bourdieu (1986) defined social capital as the resources accessible via one's network of relationships. In their comprehensive review, Bhandari and Yasunobu (2009) define it as a collective asset centered on social relationships, characterized by shared norms, values, beliefs, trust, networks, and institutions that facilitate cooperation and collective action for mutual benefit. Social capital is characterized by the quality of community members' civic engagement and mutual obligation, which both enable sustained cross-sector collaboration, especially under conditions of uncertainty or crisis (Bhandari and Yasunobu 2009). Bourdieu's observation that social capital requires "an unceasing effort of sociability [and] a continuous series of exchanges in which recognition is endlessly affirmed and reaffirmed" highlights why cybersecurity communities cannot simply rely on static institutional relationships, and must actively cultivate trust and social capital (Bourdieu 1986, 250).

Substantial social capital fosters effective information exchange, encourages engagement, and reduces risk perception, making it easier for community members to engage with each other and coordinate their responses internally and externally during cybersecurity incidents and infrastructure crises (Alvi et al. 2024; Karačić, Marić, and Kovač 2021). In both offline and online communities, social capital may be *bonding* (fostering in-group solidarity) or *bridging* (connecting diverse groups across sectors).

Bonding social capital, as defined by Omukoba and King'ara (2024), refers to the resources and trust fostered within homogenous groups, such as professionals in the same organization or field (Alves et al. 2022). When people within an organization trust each other, they tend to share important information more openly, coordinate their actions more smoothly, and follow common rules, which in turn makes the whole system more secure. These trust-based relationships improve cybersecurity performance by supporting faster decision-making, better communication, and more consistent practices (Pigola et al. 2025). While bonding social capital is beneficial, too much of it risks reinforcing information silos and may become a barrier to external connections.

Bridging social capital, on the other hand, focuses on external cooperation among government agencies, private industry, and critical infrastructure operators (Putnam 2020; Omukoba and King'ara 2024; Karačić, Marić, and Kovač 2021). Strong external relationships can break down silos, reduce delays in threat response, and foster a more resilient and adaptive cybersecurity ecosystem.

An effective balance of bonding and bridging capital fosters networks of shared responsibility. Ultimately, social capital functions as both a trust enabler and a risk mitigator in online communities. The C-CIC was conceived as an intentional effort to cultivate bonding and bridging social capital as the foundational infrastructure for effective cyber defense.

2.4 Digital Community Design Strategies

Deliberate strategies grounded in trust and social capital are essential to ensure online platforms for coordination among government, private industry, and security professionals remain effective, cohesive, and resistant to fragmentation, misinformation, and disengagement (Collett 2021; Backman 2021).

The declining access to social capital that Putnam (2020) identifies in the digital age is a significant threat to community health, making deliberate investment in building it a necessity. Putnam argues that social networks are the "quintessential resource" for any group needing to solve complex problems or mobilize for collective action. However, Putnam also demonstrates that computer-mediated platforms are inherently poor at generating deep trust and bridging social capital that are prerequisites for effective collaboration. Similarly, Gordon and Lopez

(2019) found that, rather than enthusiasm for adoption, community-based organizations expressed ambivalence and considered technology both a help and a hindrance.

Therefore, the primary challenge for any online community platform lies in incorporating design features that intentionally "thicken community ties" and overcome the natural trust deficit of digital media. To achieve these outcomes, the following four elements served as a strategic design framework for the C-CIC pilot.

2.4.1 Guiding Objectives. *Critical Sherpas* was designed to address a fundamental paradox revealed by the *Jack Voltaic* exercises: cyber resilience depends on trust networks and social coordination, yet these networks rarely exist before they are urgently needed during a crisis. Rather than treating community formation as an ancillary benefit of technical coordination platforms, we positioned it as the primary objective: to improve cross-sector cyber response capability and effectiveness by creating a trusted network of professionals who could coordinate rapidly during incidents. However, we recognized that this operational goal could only be achieved through a secondary objective: deliberately fostering the social relationships, shared norms, and institutional connections that enable coordination at scale.

2.4.2 The Strategic Foundation: A Hybrid Ecosystem. While online communities provide robust platforms for support and continuous engagement independent of physical location, they can face challenges in achieving the depth of engagement and the strong emotional connections characteristic of in-person interactions. As numerous studies suggest, effective modern-day professional communities are not purely virtual or entirely in-person. They are intentionally designed as hybrid ecosystems with enhanced capacities to leverage the strengths of both modalities to create more resilient, engaged, and effective professional networks (Alves et al. 2022; Ghamrawi 2022; Shaw et al. 2022; Borowiec et al. 2021).

While virtual work can prevent some conflicts, in-person interactions are vital for building deeper trust, resolving complex issues, and bridging gaps between subgroups. Integrating periodic in-person workshops into a virtual framework can therefore make collaborations more robust and enhance community cohesion (Alves et al. 2022; Gläsener, Afflerbach, and Weibel 2014). Research into blended learning environments indicates that combining digital and in-person educational strategies enhances engagement and learning outcomes (Namyssova et al. 2019). These blended approaches ensure that community members develop strong interpersonal relationships and trust, which are critical for effective collaboration in high-stakes environments.

Online platforms are especially effective at maintaining and expanding "weak ties"; non-hierarchical connections that go beyond face-to-face interactions, allowing individuals to assess the needs, motives, and actions of their counterparts from different organizational backgrounds and cultures, thereby bridging social capital (Granovetter 1973; Markley and

Franke 2020). Since these online interactions often lead to face-to-face meetings, online and offline community engagement become mutually reinforcing (Bruckman 2022). Millington (2021) emphasizes the importance of keeping conversations active and creating ongoing content to sustain member interest. Hosting and facilitating both online and offline events are powerful ways to keep the community vibrant.

2.4.3 Pillars of Community Trust: Governance, Culture, and Operations. Trust in an online community is rooted in transparent governance; users must understand how decisions are made and feel confident that rules are applied fairly. Clearly defined platform policies, security measures, and participation guidelines affect how users assess the platform's credibility (Collett 2021; Tian et al. 2022). Regular, open communication from platform administrators reinforces reliability (Backman 2021).

Establishing clear ethical guidelines for engagement discourages harmful behavior, misinformation, and security breaches. Active moderation and conflict resolution mechanisms prevent distrust from spreading by addressing disputes early, fairly, and transparently (Kwasek and Kocot 2023). Public reporting on cybersecurity practices builds trust by demonstrating accountability and commitment to best practices (Alvi et al. 2024; Collett 2021). Building a culture of collective responsibility in which users report suspicious activity, follow security best practices, and mentor others creates a resilient, self-sustaining trust ecosystem (Kwasek and Kocot 2023).

Users are more likely to engage when they feel valued and respected (Kwasek and Kocot 2023). Community trust thrives in an environment where diverse voices are included, contributions are recognized, and conflicts are resolved fairly (Collett 2021). Shin et al. (2024) found that a lack of feedback loops and participants' doubts that their voice made any difference in policy decisions impacted sustained engagement with civic platforms. Rewarding positive contributions and engagement by establishing recognition systems, acknowledging key insights, and promoting trusted members increases user commitment and strengthens those weak ties that build necessary social capital (Harrigan et al. 2021; Tian et al. 2022).

In addition to rewards and recognition, well-aligned incentives are crucial. Non-financial incentives can include professional development and networking opportunities. Professional development credits can be earned through training, short courses, lectures, or other live events offered by affiliated organizations. Networking opportunities help build bridging social capital by strengthening relationships between agencies and organizations. Engagement beyond crises, such as networking events, informal discussions, and shared learning initiatives, keeps trust relationships active and sustained over time (Karačić, Marić, and Kovač 2021).

Operationally, trust is best tested and strengthened before a crisis occurs. Pre-established (and practiced) crisis communication protocols ensure that stakeholders know who to trust

and where to get accurate information during cyber incidents (Backman 2021). Fischer-Preßler, Bonaretti, and Bunker (2024) found that sustained engagement was a challenge due to the need for training and different decision hierarchies across organizations. By engaging members in simulated cybersecurity incidents and collaborative problem-solving activities like *Jack Voltaic*, communities strengthen resilience and build trust networks that can be leveraged in real emergencies (Backman 2021). Collaborative training enhances cross-sector trust and improves communication and coordination between government agencies, private entities, and infrastructure operators (Collett 2021). Scenario-based trust-building activities, such as joint threat assessments or shared red-team exercises, help stakeholders build confidence in each other's expertise and decision-making capacity (Backman 2021).

Building trust in an online C-CIC requires deliberate effort, strong governance, secure identity verification, ethical leadership, and active participation. Transparency, clear policies, and verified reputation systems create an environment where stakeholders feel confident in engaging and sharing information. Additionally, ongoing security training, pre-crisis relationship-building, and collaborative cybersecurity exercises hone trust and resilience under crisis conditions. By fostering a culture of responsibility, reliability, and shared security, online C-CICs can enhance cyber resilience, cross-sector collaboration, and coordinated cybersecurity efforts.

2.4.4 Core Platform Requirements: Functional and Security Features. Vetting new users to ensure congruence of values and fit for the community is essential for trust-building, especially in communities dealing with sensitive cybersecurity concerns. User authentication, peer validation, and platform reputation scores can help mitigate misinformation, prevent impersonation, and counter bad-faith actors (Alvi et al. 2024; Karačić, Marić, and Kovač 2021). Multi-factor authentication (MFA), social authentication, and identity verification prevent unauthorized access to sensitive discussions (Wu, Edwards, and Das 2022). Reputation-based trust models, where users build credibility through peer ratings, expert endorsements, and their history of contributions, help establish and support trusted community leaders (Wu, Edwards, and Das 2022; Tian et al. 2022).

Certification systems (Karačić, Marić, and Kovač 2021) and role-based access to information channels (where verified cybersecurity experts can be distinguished from general participants) ensure that users can assess the reliability of shared information (Wu, Edwards, and Das 2022). Trust grows when members perceive the platform as a reliable source of actionable insights and secure intelligence sharing. Implementing best practices to prevent leaks, misinformation, or exploitation by malicious actors is critical for building and maintaining high levels of trust (Collett 2021). Encouraging controlled information sharing, for example, through tiered access levels, encrypted discussions, and secure document exchange protocols, protects sensitive data while maintaining transparency (Wu, Edwards, and Das 2022). Cybersecurity training

and peer-led knowledge sharing help bridge the gap between technical experts and non-technical stakeholders, increasing confidence in shared information (Kwasek and Kocot 2023). Ultimately, these technical features act as the digital scaffolding that supports the social architecture of the C-CIC, converting abstract trust into actionable security coordination.

In summary, the literature provides valuable insights into the benefits and challenges of building trust and social capital in online communities, particularly for high-stakes professional domains like cybersecurity. Practical questions, however, remain about how these principles translate into actual community-building efforts. Guided by input and feedback from C-CIC stakeholders, we set out to test these concepts in practice by designing, implementing, and beta testing a pilot community as described in the following section.

3 METHODOLOGY AND PILOT IMPLEMENTATION

The primary focus of the *Critical Sherpas* pilot study was to explore how an intentionally designed community could improve the cyber resilience of critical infrastructure. The goal of the pilot was to create a resilient, cross-sector, trust-based online community. It was designed to strengthen professional networks and processes, and to integrate key local actors into a structured virtual community with defined engagement strategies. Through a connection with our partner SherpaWerx, we enlisted the support of the Atlanta chapter of the Armed Forces Communications & Electronics Association (AFCEA) [1] to raise awareness and recruit participants. We intend for the pilot to serve as a test case for a scalable framework that could be replicated by other municipalities, counties, and states, with the long-term vision of feeding into a resilient, national critical infrastructure protection network.

The research team engaged stakeholders and reviewed technology platforms to assess critical security needs, existing capacities, interdependencies, the potential impact of disruptions, and existing protection measures. We employed a multi-phase iterative design approach to develop and test an intentional online community platform for our pilot in metro Atlanta.

3.1 Stakeholder Needs Assessment

Interviews. We conducted eight semi-structured interviews with members of the Atlanta critical infrastructure community and participants in a Jack Voltaic round table facilitated by the Army Cyber Institute. Interviewees represented government agencies, private sector organizations, academic institutions, and nonprofit entities. Half were executive-level members of the cybersecurity community, and the remaining were senior academics in cybersecurity, cyberlaw, business law, and ethics. The purpose of the interviews was to identify common coordination challenges to inform platform requirements. The interviews were conducted online and lasted no more than one hour. The interview guide included five baseline questions

1. https://www.afcea.org/

(outlined below). Following a semi-structured approach, interviewers also asked additional follow-up questions when needed.

- What websites do you find useful for your job and your organization?
- Where do you go to get your information regarding the industry?
- What do you need that you do not find in other platforms?
- Where do you find and share best practices?
- Who else do you think should be invited into the community?

We reviewed the websites listed and the resources mentioned by our interviewees to see similarities and differences with the initial architecture of the portal. Question 3 was essential in determining gaps to be filled. Question 4 when compared across disciplines allowed us to see knowledge and sharing gaps. Question 5 aimed to broaden our understanding of who is important to have in a cyber critical infrastructure community.

The purpose of this initial needs assessment was to identify areas of overlap and siloing and to adapt the platform to meet the community's needs. We used respondents' feedback to adapt and restructure the portal's architecture and to front-load information that might be useful to those who are not aware of the available resources.

Stakeholder interviews consistently emphasized the need for stronger mechanisms to connect and engage stakeholders, noting that trust and personal relationships are foundational for rapid, coordinated response. Community engagement platforms, when paired with standardized response protocols, can ensure that key players are familiar with one another and can act decisively during incidents. A centralized information repository emerged as a priority to overcome information silos, with participants seeking a single location that aggregates threat intelligence, vendor recommendations, wargame resources, and vetted tools. Respondents viewed public education initiatives as critical for building a culture of shared responsibility, improving awareness from leadership to junior staff.

Enhanced resource connectivity and secure geographic mapping of critical infrastructure were also top needs. Interviewees highlighted that cascading impacts like power outages halting water and gas flow are poorly understood across sectors, underscoring the value of tools that visualize interdependencies and supply chains. They also recommended shared calendars and discussion forums to further support collaboration, allowing stakeholders to identify gaps, share best practices, and develop collective resilience strategies. Together, these needs point to a portal that functions not just as an information hub but as an active, trusted community for cross-sector coordination.

Online Survey. We distributed an online survey in April 2024 to Metro Atlanta critical infrastructure protection professionals about the effectiveness of existing coordination efforts and organizational policies, and respondents' willingness to participate in a C-CIC. Survey

distribution leveraged professional networks, AFCEA chapters, and stakeholder referrals to reach diverse sectoral representation. The survey instrument comprised twelve questions combining open-ended and closed-ended formats. It also collected organizational demographics including sector affiliation and information on existing critical infrastructure policies or plans. Key questions included are presented in Table 1.

Table 1. Key survey questions and response formats

Survey question	**Format**
What are the biggest threats and needs for critical infrastructure protection in metro Atlanta? (up to three responses)	Open-ended
How would you assess the effectiveness of current practices to coordinate efforts among individuals and organizations involved with the protection and security of civilian critical infrastructure in metro Atlanta?	Five-point Likert scale from *very effective* to *very ineffective*
How could coordination be improved?	Open-ended
Would you or your organization be interested in participating in a Cyber Critical Infrastructure Community for metro Atlanta?	Yes/No

In total, 25 cyber professionals from a range of sectors responded to the survey, including private industry (n=15), academia (n=3), nonprofits (n=2), and government agencies or military (n=3). Asked about existing coordination efforts, only nine respondents stated their organization maintained comprehensive critical infrastructure policies, plans, and designated points of contact. Coordination effectiveness received mixed assessments, with a slight majority (n=13) rating efforts as "somewhat or very effective" while the remainder rated coordination effectiveness as "somewhat or very ineffective" (n=6), or "neither effective nor ineffective" (n=6). These findings, along with interview insights, revealed both coordination gaps and receptivity to new coordination approaches, providing empirical grounding for the design of the C-CIC portal.

These findings from interviews and surveys informed the C-CIC pilot design. Specific needs articulated by respondents indicated a strong desire for centralized threat intelligence, secure spaces for sensitive information sharing, common event calendars, and tools for visualizing critical infrastructure interdependencies.

3.2 Technology Platform Selection

Platform Benchmarking. We conducted an exploratory benchmarking analysis of nine commonly used online engagement technologies to inform our platform selection. These included conflict resolution platforms, professional networking platforms, and virtual collaboration platforms. We analyzed platform services, customization capabilities, and engagement mechanisms to understand their functionality and identify gaps relevant to identified C-CIC needs. The exploratory benchmark revealed several patterns across platform types.

The inclusion of conflict-resolution and peacebuilding platforms (Digital Peacebuilding Community of Practice, ConnexUs, Platform 4 Dialogue) reflected our theoretical premise that cybersecurity is inherently about conflict prevention and responsiveness, and that established peacebuilding concepts and practices for building trust could inform approaches to limiting or eliminating conflict during cyber crises. However, these platforms often contained outdated or inactive content, with many sites showing no recent updates or few resources. This pattern of content stagnation highlighted the challenge of sustaining engagement in online communities of practice without active management or regularly refreshed content.

Professional platforms (LinkedIn groups, IEEE Cybersecurity Community, ISACA Engage) host numerous groups dedicated to cybersecurity professionals but they generally can not be customized and restrict access to platform members only. While LinkedIn is home to highest concentration of cybersecurity-focused groups among the platforms reviewed, the members-only access model and lack of customization options limited its utility for building locally-focused communities with controlled access tiers. IEEE Cybersecurity Community and ISACA Engage similarly prioritize global professional networking over local coordination needs.

Collaboration platforms (Slack and Discord) offered different functionality, existing primarily to facilitate discussions rather than providing additional content such as information repositories or structured resources. While these platforms excel at enabling real-time communication, they lack the integrated resource-sharing, event coordination, and professional development tools identified as priorities in our stakeholder interviews. Across all platform categories, we observed that most existing solutions prioritize global networking over local coordination and lack geographic customization capabilities. It proved difficult to assess whether these communities were effective, or the extent to which they were utilized, because visibility is restricted to members only. Critically, none of the platforms in the benchmark combined local geographic focus, customizable access controls, integrated resource repositories, event coordination, and professional development tools in a single solution.

The benchmarking analysis, informed by specific needs articulated in our stakeholder interviews and surveys, justified the selection and development of a purpose-built platform.

Platform Selection. The C-CIC portal was implemented using *Mighty Networks*, a cloud-based community platform that provides integrated discussion forums, event hosting, resource sharing, and member management capabilities (Mighty Networks 2024a). *Mighty Networks* was selected based on established evaluation criteria for community platforms, including native feature integration, mobile accessibility, customization options, and scalability potential (Mighty Networks 2024b). Out of the box, the platform offers key functionalities identified as useful in our stakeholder interviews: private organizational subgroups with controlled access, integrated event calendars, resource libraries, and member verification systems.

3.3 C-CIC Design and System Architecture

The portal design integrated theoretical principles from community building literature with empirical needs identified through stakeholder interviews and survey responses. The C-CIC portal serves a hybrid digital community featuring knowledge exchange tools, private organizational subgroups, event coordination capabilities, and resource repositories.

The cloud-based technical infrastructure of *Mighty Networks* enables both web browser access and native mobile applications for iOS and Android devices, enabling cross-platform engagement essential for busy professionals. The platform's "spaces" architecture allows for flexible community organization, with different access levels for general community discussions, sector-specific working groups, and restricted information sharing areas. Although the platform offers built-in analytics capabilities for tracking member engagement, we used it primarily for interacting with users and monitoring community growth.

The platform housing the portal had architectural limitations, including security gaps which forced us to create a two-step referral and admission process supported by user monitoring and member vigilance. Due to time constraints and the limited number of adopters we were not able to fully implement community-building best practices with the C-CIC portal.

3.4 Pilot Beta Testing

A dozen cybersecurity professionals, selected from our initial needs assessment and referrals, accepted invitations to participate in structured virtual beta testing sessions. Four sessions captured user experience data, design recommendations, and functionality assessments, informing subsequent platform modifications to enhance navigation, access controls, and user guidance systems. Beta test users provided real-time feedback via screen-sharing sessions with the testing team. Users were given rudimentary navigation instructions and an initial overview of the portal. They were then asked to navigate it on their own, with testing team members available to assist and answer questions. Feedback was analyzed to assess the portal's usability and potential utility.

In general, the feedback reflected a tension between ease of use and strong security. Test users appreciated having strong security and controlled access, but they also needed the platform to be easy to navigate and quick to use during fast-moving situations. Some test users expressed strong enthusiasm for the platform's cross-sector information-sharing capabilities and its controlled-access features for sensitive discussions. Participants from a government agency expressed a desire for a portal that would give counties a way to access information and for the agency to disseminate information to them.

Although pilot adoption fell short of established benchmarks for sustained engagement, feedback revealed two categories of potential enhancements: 1) the need for enhanced user

guidance on information sharing protocols and privacy controls, and 2) improved user experience for section accessibility, joining processes, and feature functionality.

4 DISCUSSION

The experience of the C-CIC pilot highlights a fundamental challenge in cyber resilience community-building: initial enthusiasm among stakeholders does not automatically translate into sustained engagement. This pattern suggests that simply transplanting traditional community-building strategies into cybersecurity contexts may be insufficient. Instead, the findings from our pilot point to the need for tailored approaches that address the unique barriers to ongoing participation in cyber-focused communities such as the sensitivity of information, the demands on professionals' time, and the complexities of trust and verification in digital environments. Interpreting these findings, it becomes clear that fostering lasting engagement in cyber resilience initiatives requires rethinking conventional models and developing new frameworks that are responsive to the specific needs and constraints of cybersecurity practitioners.

Our survey results revealed that nearly half of the respondents rated current efforts as only "somewhat effective," while only one respondent considered them "very effective." These results suggest room for coordination improvement, though the limited sample size and engagement levels prevent broad generalization. Have stakeholders come to accept suboptimal coordination as an acceptable baseline performance? Addressing this possibility in future research could help clarify how organizational expectations influence collaborative performance in cybersecurity contexts.

4.1 Community Engagement: The Critical Mass Problem

The most significant challenge of the *Critical Sherpas* pilot was achieving sustainable engagement. With only 25 early adopters from the target metropolitan area population, the portal fell short of Millington's (2021) critical mass benchmarks: 100 contributing members per month, 300 monthly posts, and 10 new registrations per day. Consistent with findings in the broader literature on leadership and sustainability of online communities (Kraut et al. 2012; Johnson, Safadi, and Faraj 2015), the pilot's reliance on a single community champion, AFCEA Atlanta (via a connection with our partner SherpaWerx), rather than a larger number of stakeholders, proved limiting.

Engert et al. (2023) show that sustained engagement on digital platforms depends on strengthening five antecedents: clear platform rules, a compelling value proposition, active platform agents, alignment with user needs, and visible contributions from complementors (members offering different perspectives that enhance the value of each other's participation). These enable the core behaviors of sharing information, connecting with others, and coordinating efforts. While these factors and behavioral objectives were all considered in

the design of the C-CIC pilot, engagement metrics are needed to understand how specific design choices affect changes in these behaviors and overall community engagement. Future research should test different engagement approaches and track participation longitudinally to determine which methods are most effective and sustainable.

4.2 Designing for Trust: The Usability-Security Tension

Stakeholders and participants uniformly highlighted the importance of clear information-sharing protocols and strong privacy controls, underscoring the challenge of calibrating trust in environments where transparency itself can heighten vulnerability. Prior research suggests that in professional and emergency response networks, trust calibration depends on both the perceived credibility of information sources and the robustness of governance mechanisms that protect against misuse. Backman (2021) emphasizes that pre-established trust networks enable rapid, secure information exchange during crises, while Alvi et al. (2024) and Wu, Edwards, and Das (2022) note that effective trust mechanisms must balance institutional assurance with interpersonal confidence to reduce risk and support collaboration. This means that C-CIC platform design must mirror these trust architectures—embedding clear validation systems, transparent but bounded communication channels, and flexible privacy controls that sustain confidence without compromising security.

Balancing the tension between ease of use and strong security is necessary in cybersecurity and critical infrastructure protection, where mistakes can have serious consequences (Di Nocera, Tempestini, and Orsini 2023). This highlights a central challenge: the system must protect sensitive information while still allowing people to work together smoothly and efficiently. Our platform comparison suggests that large, general-purpose systems often focus on reaching many users rather than supporting careful, high-quality coordination. In contrast, our pilot indicates that a more specialized, security-focused platform may be necessary for the kind of precise, trust-based collaboration that C-CICs depend on. The enthusiasm for features that enable private subgroups with controlled access suggests that stakeholders recognize the need for bridging social capital and building nuanced trust within the broader community.

4.3 Incentives for Sustained Engagement

The lack of formal incentives, including rewards, recognition, or professional development credits likely contributed to the limited engagement in the C-CIC pilot. Instead, we relied on intrinsic motivation, which proved insufficient against the competing time demands of cybersecurity professionals. Our findings parallel tensions documented in other security-sensitive professional networks. Like intelligence communities that must balance collective learning against "need to know" secrecy protocols (Rusho et al. 2025), and healthcare information exchanges navigating privacy constraints, cyber infrastructure communities face inherent contradictions between the openness required for effective knowledge sharing and

the competitive or confidentiality pressures that inhibit it. Research on "coopetition" networks demonstrates that formal coordination mechanisms and technology-enabled trust-building become essential when standard community assumptions of voluntary, open participation cannot apply (Tsai 2002; Randolph, Hu, and Silvernail 2020).

4.4 Implications for Theory and Practice

While *Critical Sherpas* faced expected challenges common to new online communities, the pilot surfaced valuable insights that align closely with findings of Kraut et al. (2012) on the importance of clearly defined objectives and competitive differentiation. The project was intentionally designed to foster organic growth, and while this approach yielded enthusiastic engagement from early adopters and strong initial partnerships, it also revealed the need for more structured facilitation, diversified leadership, and more precise articulation of the platform's unique value. These lessons reflect the natural evolution of a complex, multi-sector initiative and offer a strong foundation for refining future efforts. By aligning more closely with proven strategies such as establishing a clear purpose, building referral systems, and defining a competitive niche, future iterations of the C-CIC portal can be positioned for broader adoption and sustained impact.

One consideration pertaining to cyber and critical infrastructure communities is whether the inclusion and handling of highly sensitive information is appropriately accounted for, both theoretically and practically. Further research is necessary to determine if design modifications are needed for more effective connection, coordination, and collaboration between professionals and organizations who need to use and share sensitive information to fulfill their respective responsibilities. Existing community theory, particularly as applied to information sharing and analysis centers (ISACs) and computer emergency response teams (CERTs), focuses extensively on solving the information-sharing dilemma: the collective action problem of exchanging sensitive threat intelligence (Gillard et al. 2023; Stein 2023). However, this framing may be misaligned with the primary value proposition of a geographically bounded C-CIC.

The metro Atlanta-focused pilot suggests that the primary value of C-CICs lies in establishing relational infrastructure that exists independent of transactional data exchange. Members do not necessarily need to share proprietary breach data to benefit from understanding regional roles, establishing face-to-face familiarity with counterparts, and proactively building bonding and bridging social capital in the community. These relationships enable rapid, trust-based coordination when digital channels fail or time pressures prohibit formal vetting of personnel and information. This distinction aligns with emergency management literature on "swift trust" (Wong 2013), which demonstrates that crisis coordination depends less on information transparency than on pre-defined roles and prior relationship-building. Unlike virtual ISACs where value is measured by intelligence-sharing volume, the success of geographic C-CICs

is whether a utility CISO knows precisely whom to call when a regional attack occurs, and trusts that person will answer.

Standard community theory's emphasis on openness and reciprocity thus requires modification: in security-sensitive contexts, affective social capital (familiarity, affect, emotional bonds) may be cultivated without solving the cognitive social capital dilemma (informational trust, data reciprocity). The argument underlying the C-CIC model is that these can be decoupled.

Additional findings from the C-CIC pilot suggest that applying community resilience frameworks to the cyber domain requires significant adaptation. Unlike face-to-face communities, where social capital is reinforced through physical proximity and chance encounters, cyber communities operate in an environment of invisible relationships. In this context, resilience does not emerge organically; it must be engineered. Our research indicates that digital trust differs fundamentally from physical trust; it is fragile, prone to siloing, and heavily dependent upon verification. Because online bonding can easily become insular, bridging capital (the connection between diverse sectors) must be deliberately fostered through structured interventions like cross-sector forums, shared calendars, and trust-building exercises.

These theoretical distinctions have immediate practical implications. While community resilience principles offer a helpful starting point, our pilot demonstrates that grassroots volunteerism alone is insufficient for sustaining a C-CIC. The unique constraints of the cybersecurity profession, including the high sensitivity of information, reputational risk, and extreme time pressure, mean that these communities cannot function on intrinsic motivation alone. We argue that cyber community building must transition from a volunteer-driven model to an institutional infrastructure model. Sustainable C-CICs require enterprise-grade technical infrastructure, robust security protocols, and, crucially, dedicated professional facilitation. Just as physical infrastructure requires maintenance crews, digital social infrastructure requires community managers to verify identities, curate threat intelligence, and maintain the 'we-consciousness' that prevents engagement drop-off.

These needs raise important questions regarding scalability. If achieving critical mass is challenging within a single metropolitan area with dense professional networks, scaling such initiatives to regional, national, or international levels presents exponentially more barriers. Future research should investigate whether a federated model connecting local, high-trust C-CICs is more effective than a monolithic national platform. Ultimately, the beta test validated that while trust and social capital drive cyber resilience, intentionally designed communities must be carefully engineered and require institutional investment to function. Cyber community building should not be viewed as a low-cost networking experiment, but rather as a well-funded, well-resourced imperative for national security and resilient emergency preparedness infrastructure.

CONCLUSION

The C-CIC pilot advances our understanding of cyber resilience by demonstrating that adapting community-building principles from face-to-face to online contexts can improve cyber critical infrastructure coordination. However, successful implementation requires significant modification to address the unique constraints of cybersecurity environments. Our Atlanta-based *Critical Sherpas* pilot provides empirical evidence that stakeholder demand for improved cyber coordination exists and that effective coordination through an online community platform design is achievable. However, sustainable engagement demands professional-grade facilitation and institutional investment rather than volunteer-driven approaches. This finding has important implications for how we conceptualize cyber resilience as both a theoretical framework and a practical imperative.

For practitioners and policymakers, this research suggests that effective cyber critical infrastructure communities should be treated as an essential coordination infrastructure that requires dedicated funding, professional management, and enterprise-level technical coordination. Organizations and agencies investing in cyber resilience initiatives should budget for sustained community facilitation, recognizing that busy cybersecurity professionals need well-designed and easily accessible structured engagement opportunities that clearly add professional value rather than additional volunteer commitments. The success of such initiatives may depend on integrating community building into existing frameworks for professional development and emergency preparedness, and forming industry associations where participation can be formally recognized and resourced.

Based on these findings, future cyber community initiatives should implement specific design principles, including multi-sectoral stakeholder teams instead of single champions, structured referral pathways for sustained growth, and hybrid approaches that combine online platforms with in-person events and trust-building activities. Building on the theoretical framework distinguishing relational from cognitive social capital, geographically bounded cyber communities appear optimally positioned to cultivate the affective bonds, role familiarity, and face-to-face relationships that enable rapid crisis coordination, a function distinct from the information-sharing mandate of national-scale ISACs or CERTs. The integration of structured referral pathways as part of outreach, awareness-raising, and engagement activities can enhance participation and strengthen community ties beyond what can be achieved through purely digital approaches. Broad, inclusive partnerships with cyber stakeholders across sectors will be essential for achieving the scale and sustainability that voluntary approaches cannot provide, requiring institutional commitment rather than relying on individual enthusiasm alone.

The broader implications for a national cybersecurity strategy are significant. Since cyber threats increasingly require systematic and coordinated community responses, building

resilient cyber communities becomes a matter of national security, and infrastructure investment must go far beyond optional networking enhancement. Future research should examine optimal resource allocation models for cyber community initiatives, evaluate the effectiveness of different institutional partnership frameworks, and develop metrics for assessing community-level cyber resilience outcomes. The path forward requires treating cyber community building as seriously as we treat other forms of critical infrastructure protection. Sustained investment, professional expertise, and the recognition that community resilience is a public good become essential for effectively protecting national security.

ABOUT THE AUTHORS

Dr. Anne M. Chance directs Solution Labs for TRENDS Global. Her research focuses on historical identity, personal values, and ethno-territoriality. Dr. Chance has a Ph.D. in International Conflict Management, Peacebuilding, and Development, a Master's Degree in Cultural Preservation. She is currently developing vertically integrated program labs that teach resiliency practices to emerging professionals.

Dr. Volker Franke is Professor of Conflict Management at Kennesaw State University and Founder and Executive Director of TRENDS Global, a 501c3 nonprofit, dedicated to research and capacity strengthening in community-focused peacebuilding and conflict transformation (https://trendsglobal.org). Dr. Franke has extensive experience in research and capacity building in conflict management and adaptive peacebuilding.

Timo Zwarg is a PhD Candidate in International Conflict Management, Peacebuilding, and Development at Kennesaw State University. Mr. Zwarg holds a Master of Science in Peace and Security from the University of Hamburg. His research focuses on decolonial practices, participatory action, and community peacebuildling.

ACKNOWLEDGMENTS

The *Critical Sherpas* C-CIC pilot study team included researchers from Kennesaw State University, SherpaWerx, and TRENDS Global. The pilot was financially supported by the Army Cyber Institute at West Point.

REFERENCES

ACI (Army Cyber Institute). 2021a. *Jack Voltaic 3.0: Cyber Research Report - Prepare | Prevent | Respond.* Technical report. https://cyber.army.mil/Portals/3/Documents/JackVoltaic/3.0/JackVoltaic_Executive_Summary_3.0.pdf.

Alves, M., I. Dimas, P. Lourenço, T. Rebelo, V. Peñarroja, and N. Gamero. 2022. "Can Virtuality Be Protective of Team Trust? Conflict and Effectiveness in Hybrid Teams." *Behaviour & Information Technology* 42 (7): 851–68. https://doi.org/10.1080/0144929X.2022.2046163.

Alvi, Tariq Hameed, Samia Tariq, Amad Rashid, and Maryyam Qasim Khan. 2024. "Trust Mechanisms in the Sharing Economy." *Pakistan Business Review* 26 (3): 228–51. https://doi.org/10.22555/pbr.v26i3.1284.

Army Cyber Institute. 2018. *Jack Voltaic 2.0: Threats to Critical Infrastructure - Executive Summary.* Technical report. Army Cyber Institute, United States Military Academy. https://cyber.army.mil/Portals/3/Documents/JackVoltaic/JV2_Exsum_FINAL.pdf.

Army Cyber Institute. 2021b. *Jack Voltaic 3.0: Executive Summary - Increasingly Connected, Ready to Respond.* Technical report. Army Cyber Institute, United States Military Academy. https://cyber.army.mil/Portals/3/Documents/JackVoltaic/3.0/JackVoltaic_Executive_Summary_3.0.pdf.

Army Cyber Institute. 2022. *Planning Playbook: Jack Voltaic®. Version 1.1.* Technical report.

Backman, Sarah. 2021. "Conceptualizing Cyber Crises." *Journal of Contingencies and Crisis Management* 29 (4): 429–38. https://doi.org/10.1111/1468-5973.12347.

Bhandari, Humnath, and Kumi Yasunobu. 2009. "What Is Social Capital? A Comprehensive Review of the Concept." *Asian Journal of Social Science* 37 (3): 480–510. https://doi.org/10.1163/156853109X436847.

Björck, Fredrik, Henric Johnson, Johan Johnson, and Martin Löf. 2015. "Cyber Resilience: Fundamentals for a Definition." In *Availability, Reliability, and Security in Information Systems,* edited by Alvaro Rocha, Ana Maria Correia, Sandra Constanzo, and Luis Paulo Reis, vol. 315. Advances in Intelligent Systems and Computing. Springer International Publishing. https://doi.org/10.1007/978-3-319-16486-1_31.

Bohill, Ruth Rewa. 2010. "Intentional Communities: Ethics as Praxis." PhD diss., Southern Cross University. https://researchportal.scu.edu.au/esploro/outputs/doctoral/Intentional-Communities--Ethics-as-Praxis/991012821645102368.

Borowiec, Katrina, Deoksoon Kim, Lizhou Wang, Juli Kim, and S. Wortham. 2021. "Supporting Holistic Student Development Through Online Community Building." *Online Learning* 25 (4): 154–71. https://doi.org/10.24059/olj.v25i4.2882.

Bourdieu, Pierre. 1986. "The Forms of Capital." In *Handbook of Theory and Research for the Sociology of Education*, edited by John G. Richardson. Greenwood Press.

Bruckman, Amy S. 2022. *Should You Believe Wikipedia?: Online Communities and the Construction of Knowledge.* 1st. Cambridge University Press. https://doi.org/10.1017/9781108780704.

Castelfranchi, C., R. Falcone, and F. Marzo. 2006. "Being Trusted in a Social Network: Trust as Relational Capital." In *Trust Management. iTrust 2006,* edited by K. Stølen, W.H. Winsborough, F. Martinelli, and F. Massacci, vol. 3986. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11755593_3.

Chance, Anne M. 2023. "Inscribing Violence: Quantifying the Impact of World Heritage Site Inscription on Direct and Structural Violence." PhD diss., Kennesaw State University. https://digitalcommons.kennesaw.edu/incmdoc_etd/51.

Collett, Robert. 2021. "Understanding Cybersecurity Capacity Building and Its Relationship to Norms and Confidence Building Measures." *Journal of Cyber Policy* 6 (3): 298–317. https://doi.org/10.1080/23738871.2021.1948582.

Di Nocera, Francesco, Giorgia Tempestini, and Matteo Orsini. 2023. "Usable Security: A Systematic Literature Review." *Information* 14 (12): 641. https://doi.org/10.3390/info14120641.

Engert, Martin, Julia Evers, Andreas Hein, and Helmut Krcmar. 2023. "Sustaining Complementor Engagement in Digital Platform Ecosystems: Antecedents, Behaviours and Engagement Trajectories." *Information Systems Journal* 33 (5): 1151–1185. https://doi.org/10.1111/isj.12438.

Erickson, M., and T. Harvey. 2023. "A Framework for a Structured Approach for Formulating a Trauma-Informed Environment." *Journal of Education* 203 (3): 666–677. https://doi.org/10.1177/00220574211046811.

Fischer-Preßler, Diana, Dario Bonaretti, and Deborah Bunker. 2024. "Digital Transformation in Disaster Management: A Literature Review." *The Journal of Strategic Information Systems* 33 (4): 101865. https://doi.org/10.1016/j.jsis.2024.101865.

Galtung, J. 1969. "Violence, Peace, and Peace Research." *Journal of Peace Research* 6 (3): 167–191. http://www.jstor.org/stable/422690.

Galtung, J. 1990. "Cultural Violence." *Journal of Peace Research* 27 (3): 291–305.

Galtung, J., and T. Höivik. 1971. "Structural and Direct Violence: A Note on Operationalization." *Journal of Peace Research* 8 (1): 73–76. https://doi.org/10.1177/002234337100800108.

Ghamrawi, Norma. 2022. "Teachers' Virtual Communities of Practice: A Strong Response in Times of Crisis or Just Another Fad?" *Education and Information Technologies* 27 (5): 5889–915. https://doi.org/10.1007/s10639-021-10857-w.

Gillard, S., D. Percia David, A. Mermoud, and T. Maillart. 2023. "Efficient Collective Action for Tackling Time-Critical Cybersecurity Threats." *Journal of Cybersecurity* 9 (1): tyad021. https://doi.org/10.1093/cybsec/tyad021.

Gläsener, Katharina, Thomas Afflerbach, and Antoinette Weibel. 2014. "Trust and Distrust in Hybrid Virtual Teams: Perceptions of Trustworthiness across Subgroup Boundaries." In *8TH FINT/EIASM Conference on Trust within and between Organisations.* https://www.alexandria.unisg.ch/handle/20.500.14171/86160.

Gordon, Eric, and Rogelio Alejandro Lopez. 2019. "The Practice of Civic Tech: Tensions in the Adoption and Use of New Technologies in Community Based Organizations." *Media and Communication* 7 (3): 57–68. https://doi.org/10.17645/mac.v7i3.2180.

Government Accountability Office. 2021. *SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response,* April 22, 2021. https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.

Granovetter, Mark S. 1973. "The Strength of Weak Ties." *American Journal of Sociology* 78 (6): 1360–1380. https://doi.org/10.1086/225469.

Harrigan, Maggie, Kim Feddema, Shasha Wang, Paul Harrigan, and Emmanuelle Diot. 2021. "How Trust Leads to Online Purchase Intention Founded in Perceived Usefulness and Peer Communication." *Journal of Consumer Behaviour* 20 (5): 1297–312. https://doi.org/10.1002/cb.1936.

Hiscox. 2023. *Hiscox Cyber Readiness Report 2023.* Technical report. https://www.hiscox.com/documents/Hiscox-Cyber-Readiness-Report-2023.pdf.

Hossain, Sk Tahsin, Tan Yigitcanlar, Kien Nguyen, and Yue Xu. 2024. "Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework." *Applied Sciences* 14 (13): 5501. https://doi.org/10.3390/app14135501.

Johnson, Steven L., Hani Safadi, and Samer Faraj. 2015. "The Emergence of Online Community Leadership." *Information Systems Research* 26 (1): 165–87. https://doi.org/10.1287/isre.2014.0562.

Karačić, Adriana, Ivana Marić, and Jelena Kovač. 2021. "The Importance of Service User Trust in the Collaborative Economy." In *Proceedings of the Central European Conference on Information and Intelligent Systems (Varaždin, Croatia),* 107–14.

Kraut, Robert E., Paul Resnick, Sara Kiesler, Moira Burke, and Yan Chen, eds. 2012. *Building Successful Online Communities: Evidence-Based Social Design.* MIT Press.

Kwasek, Artur, and Maria Kocot. 2023. "Organisational Agility as a Factor Determining Trust in Organisations." *Zarządzanie – Working Papers Humanitas University Management,* no. 1, 193–211. https://doi.org/10.5604/01.3001.0054.2981.

Lederach, John Paul. 2005. *The Moral Imagination: The Art and Soul of Building Peace.* New York: Oxford University Press.

Linkov, Igor, and Alexander Kott. 2018. "Fundamental Concepts of Cyber Resilience: Introduction and Overview." In *Cyber Resilience of Systems and Networks,* edited by Igor Linkov and Julia T. Richards. Springer. https://doi.org/10.1007/978-3-319-77492-3_1.

Markley, Eliza, and Volker Franke. 2020. "Snowball Networking: Making Security Cooperation more effective through Personal Communication." *Journal of Communication and Behavioural Sciences* 1 (1): 19–34.

Mighty Networks. 2024a. *Features: Community Platform for Building, Engaging & Monetizing.* https://www.mightynetworks.com/features.

Mighty Networks. 2024b. *How to Evaluate Community Platforms,* February 6, 2024. https://www.mightynetworks.com/resources/how-to-evaluate-community-platforms.

Millington, Richard. 2021. *Build Your Community: Turn Your Connections into a Powerful Online Community.* 1st. Pearson Business.

Namyssova, Gulnara, G. Tussupbekova, Janet Helmer, K. Malone, Mir Afzal, and D. Jonbekova. 2019. "Challenges and Benefits of Blended Learning in Higher Education." In *Proceedings of the 2nd International Conference on Education and Social Sciences,* 22–31.

NIST (National Institute of Standards and Technology). 2021. *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach.* NIST Special Publication 800-160, Volume 2, Rev. 1. National Institute of Standards, Technology, and the MITRE Corporation, December. https://doi.org/10.6028/NIST.SP.800-160v2r1.

NIST (National Institute of Standards and Technology). 2022. *Assessing Enhanced Security Requirements for Controlled Unclassified Information.* NIST Special Publication 800-172A. National Institute of Standards and Technology, March. https://doi.org/10.6028/NIST.SP.800-172A.

NIST (National Institute of Standards and Technology). 2024. *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach.* NIST Special Publication 800-160, Volume 2, Rev. 2. National Institute of Standards, Technology, and the MITRE Corporation. https://doi.org/10.6028/NIST.SP.800-160v2r2.

NIST (National Institute of Standards and Technology). *Resilience.* Website. https://csrc.nist.gov/glossary/term/resilience.

Norris, Fran H., Susan P. Stevens, Betty Pfefferbaum, Karen F. Wyche, and Rose L. Pfefferbaum. 2008. "Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness." *American Journal of Community Psychology* 41 (1-2): 127–150. https://doi.org/10.1007/s10464-007-9156-6.

Omukoba, Deckillah S., and George N. King'ara. 2024. "Membership in Online Groups: A Source of Bridging and Bonding Social Capital for Kenyan Youth." *Journal of the Kenya National Commission for UNESCO* 5 (1): 1–19. https://doi.org/https://doi.org/10.62049/jkncu.v5i1.221.

Pigola, Angélica, Priscila Rezende da Costa, Leonardo Vils, and Fernando de Souza Meirelles. 2025. "Enhancing Information Security Management and Performance through Social and Relational Factors: A Structural Equation Modelling Approach." *Behaviour & Information Technology* (June): 1–23. https://doi.org/10.1080/0144929X.2025.2522206.

Putnam, Robert D. 2020. *Bowling Alone: The Collapse and Revival of American Community.* Revised and Updated. Simon & Schuster.

Rahmonbek, Komron. 2025. *35 Alarming Small Business Cybersecurity Statistics for 2025,* January. Accessed October 24, 2025. https://www.strongdm.com/blog/small-business-cyber-security-statistics.

Randolph, Ryan V., Haiyan Hu, and Kevin D. Silvernail. 2020. "Better the Devil You Know: Inter-Organizational Information Technology and Network Social Capital in Coopetition Networks." *Information & Management* 57 (6): 103344. https://doi.org/https://doi.org/10.1016/j.im.2020.103344.

Rusho, Yael, Daphne R. Raban, Daniel Simantov, and Gal Ravid. 2025. "Knowledge Sharing in Security-Sensitive Communities." *Future Internet* 17 (4): 144. https://doi.org/https://doi.org/10.3390/fi17040144.

Shaw, L., Dana Jazayeri, D. Kiegaldie, and M. Morris. 2022. "Implementation of Virtual Communities of Practice in Healthcare to Improve Capability and Capacity: A 10-Year Scoping Review." *International Journal of Environmental Research and Public Health* 19 (13): 7994. https://doi.org/10.3390/ijerph19137994.

Shin, Bokyong, Jacqueline Floch, Mikko Rask, Peter Bæck, Christopher Edgar, Aleksandra Berditchevskaia, Pierre Mesure, and Matthieu Branlat. 2024. "A Systematic Analysis of Digital Tools for Citizen Participation." *Government Information Quarterly* 41 (3): 101954. https://doi.org/10.1016/j.giq.2024.101954.

Smith, Sidney. 2023. "Towards a Scientific Definition of Cyber Resilience." In *Proceedings of the 18th International Conference on Cyber Warfare and Security,* 18:379–86. 1. https://doi.org/10.34190/iccws.18.1.960.

Stein, D. 2023. "Data Insecurity Law." *Santa Clara High Technology Law Journal* 39 (4): 445–512. https://digitalcommons.law.scu.edu/chtlj/vol39/iss4/1.

Tian, Yuan, Honglei Zhang, Yifei Jiang, and Yang Yang. 2022. "Understanding Trust and Perceived Risk in Sharing Accommodation: An Extended Elaboration Likelihood Model and Moderated by Risk Attitude." *Journal of Hospitality Marketing & Management* 31 (3): 344–68. https://doi.org/10.1080/19368623.2022.1986190.

Tierney, Kathleen. 2019. *Disasters: A Sociological Approach.* Polity Press.

Tsai, Wenpin. 2002. "Social Structure of 'Coopetition' within a Multiunit Organization: Coordination, Competition, and Intraorganizational Knowledge Sharing." *Organization Science* 13 (2): 179–90. https://www.jstor.org/stable/3085992.

Wong, L. C. 2013. *Understanding 'Swift Trust' to Improve Interagency Collaboration in New York City.* Technical report. Defense Technical Information Center.

Wood, Kimberly. 2023. *Cybersecurity Policy Responses to the Colonial Pipeline Ransomware Attack.* The Georgetown Environmental Law Review, March 7, 2023. https://www.law.georgetown.edu/environmental-law-review/blog/cybersecurity-policy-responses-to-the-colonial-pipeline-ransomware-attack/.

Wu, Yuxi, W. Keith Edwards, and Sauvik Das. 2022. "SoK: Social Cybersecurity." In *2022 IEEE Symposium on Security and Privacy (SP),* 1863–1879. IEEE. https://doi.org/10.1109/SP46214.2022.9833757.

Young, Kelli. 2021. "Cyber Case Study: City of Atlanta Ransomware Incident," September 20, 2021. https://coverlink.com/case-study/city-of-atlanta-ransomware/.

Received 17 March 2025; Revised 18 November 2025; Accepted 24 November 2025