How CIP Practitioners Identify, Infer, and Validate Trust Networks:

Using SNA to Identify Evidence-Based, People-Centric Best Practices

WRITTEN BY
Michael Maloney

2026

INSTITUTE FOR HOMELAND SECURITY
SAM HOUSTON STATE UNIVERSITY

ABSTRACT

This paper is designed to help the Critical Infrastructure Protection (CIP) practitioners understand the value of trust networks and identify ways to assess and validate their own trust networks to achieve decisional advantage. This paper is designed to strike a balance between social network analysis theory and practical application. There are four fundamental conclusions of this paper:

1. CIP practitioners are inherently part of a trust network, as we define it, by virtue of their position.
2. CIP practitioners have few formal tools for assessing the quality of their trust networks and therefore have a limited ability to determine its effectiveness based upon their own biases. Employing evidence-based practices as both art and science can improve the ability of CIP practitioners to assess, validate, and improve their trust networks.
3. There are positive and negative features of trust networks; using evidence-based practices can accentuate the former and minimize the latter.
4. CIP trust networks should be assessed and validated to improve CIP decisions and therefore a valid business use case exists for CIP trust network validation activities.

Finally, we offer evidence-based practices for improving CIP trust networks, and show how trust networks can be effectively utilized for impact. [1]

[1] The opinions expressed within this paper are those of the author and do not represent any governmental agency or private corporation for which the author has worked.

Table of Contents

INTRODUCTION AND OVERVIEW

The interconnectedness of modern critical infrastructure demands information sharing across trust networks between Critical Infrastructure Protection (CIP) practitioners to preserve the integrity of systems that rely on one another for optimal functionality. Trust networks facilitate information sharing by helping individuals rapidly add trust to newly obtained information. An example of this interconnectedness is found in the winter storm that devastated Texas in 2021, initially compromising the power grid, but subsequently causing the water system to fail, resulting in $130 billion in economic repercussions (Busby et al., 2021). CIP practitioners collaborate across trust networks to safeguard the integrity of their components. These trust networks include professional organizations, informal peer networks, and working groups led by state, local, or federal partners, to name a few. The validation levels and information sharing standards vary among these networks. For instance, professional organizations often require minimal validation, while organizations governed by state, local, or federal agencies typically impose stringent membership requirements and higher information sharing standards but may come with other drawbacks. Social network analysis of these trust networks facilitates the establishment of industry-facing, evidence-based best practices for CIP practitioners when they are building their trust networks while accounting for the pros and cons of various trust networks.

Along the way, we will identify ways to assess the strength of networks, validation methods, and understand the pitfalls of trust networks.

Analytic Goals: Evidenced-based, People-Centric Practices

The goal of this analysis is to determine evidenced-based, best practices surrounding the following three questions:

1. How do CIP practitioners assess and validate their own trust networks?
2. How effective are CIP practitioners in validating their trust networks and identifying gaps therein?
3. How do CIP practitioners view the benefits and downsides of various trust networks, and how does that impact their assessments?

Before answering these questions, we must first define trust networks in the context of CIP practitioners. A dearth of literature on this subject means we must craft this definition from several sources before moving towards our analysis.

Definition of Critical Infrastructure Trust Networks:

In their seminal work on Social Network Analysis, Stanley Wasserman and Katherine Faust, while not specifically discussing trust networks, refer to cohesive networks and affiliation networks. These are useful frameworks to begin our discussion of trust networks. Wasserman and Faust define “cohesive subgroups” as subsets of actors among whom there are relatively strong, direct, intense, frequent, or positive ties” (Wasserman & Faust, 1994). In the context of CIP practitioners, this may include the chief security officer of a utility company and their regional security managers, for example. They further define affiliation networks as, “two-mode networks consisting of a set of actors and a set of events…[and] describe collections of actors rather than simply ties between pairs of actors” (Wasserman & Faust, 1994). An affiliation network in the context of CIP practitioners may be the chief security officer and their team, mentioned above, as well as a regional consortium of security practitioners that meets occasionally to share vital information or another public-private venture such as InfraGard or an Information Sharing and Analysis Center (ISEC). Highly cohesive networks will have high network density and short information paths between network members because members are connected to most other members. (see figure one). It will also have a low betweenness centrality measure, meaning that individual actors are not needed to bridge information or serve as a gatekeeper because most members of the network are connected to one another.

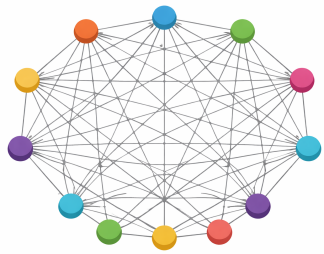

Figure 1: Cohesive Network may limit ingest of new information.

Our journey to define CIP trust networks must also be influenced by Mark Granovetter’s widely cited work on the importance of “weak ties.” In 1973, Granovetter concluded, “weak ties, often denounced as generative of alienation (Wirth 1938), are here seen as indispensable to individuals’ opportunities and to their integration into communities; strong ties, breeding local cohesion, lead to overall fragmentation” (Granovetter, 1973). But this is only true if the weak ties serve as “bridges” between strong ties. Granovetter defined a bridge as, “a line in a network which provides the only path between two points” (Granovetter, 1973). An example of a bridge in the context of CIP practitioners may be the regional security manager of a communications provider who has strong ties to several local police detectives in the communities where their company has infrastructure. This regional security manager can “bridge” trust and new information amongst the local detectives to help connect disparate data points with increased confidence to aid decision-making. In social network analysis theory, these “bridges” can be assessed by the betweenness centrality metric. (see figure two).

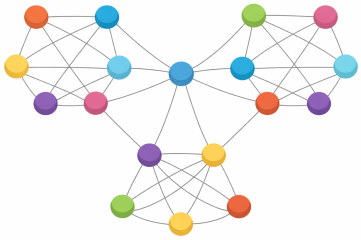

Figure 2: Weak ties may complement strong ties to enhance trust.

From Wasserman and Faust, as well as Granovetter, we can therefore begin to define a trust network in the context of CIP practitioners, as having elements of cohesive

networks and affiliation networks while being tempered by an understanding of the importance of bridges in their networks. These bridges may be individuals, events, or standing organizations.

To these theoretical underpinnings of a CIP practitioner trust network, we must also add the element of compliance and resiliency. Even before the terrorist attacks of 9/11, an ever-growing and evolving body of laws, regulations, and public-private ventures surrounding critical infrastructure has emerged. Designed to increase resilience via the establishment of standards as well as improving information sharing, these mandates and institutions further complicate our definition of a trust network. Government, in general, has tried to err on the side of not mandating information sharing but encouraging it through the establishment of institutions such as InfraGard and various ISACs, both of which were established in the 1990s. CIP practitioners must incorporate these elements into their validation frameworks for their trust networks.

Finally, we must add that CIP practitioners share and receive information for a purpose: improved decision-making. Being able to rapidly assign trust to new information to support decision-making is the point of CIP practitioners validating, assessing, and improving trust networks.

So, taking into account cohesion, the importance of weak ties as well as resiliency-driven mandates and public-private sharing networks, and the purpose of the network itself, the following definition is proposed for this discussion:

> ***CIP Practitioner Trust Network Definition: A social network consisting of both formal and informal, strong and weak ties to facilitate bona fide information flow while also allowing new information and practices to enter the network, and complying with relevant regulations and laws, designed to achieve decisional advantage.***

From this definition, we deduce that CIP trust networks are complex in nature, taking into account several variables that are often changing. They may have their roots in homophily, or the tendency for people to associate with someone like themselves, but they are guided by regulation as well as the need to be diffuse enough with weak ties to allow for new trusted information to enter the network. To put this problem in social network analysis theoretical terms, CIP practitioners must balance network density, information path length, and betweenness centrality to promote enough trusted and interdisciplinary relationships, while also allowing for enough bridges to promote new trusted information entering the network. Too much density with low betweenness may lead to groupthink; not enough density and too much betweenness may lead to information overload and low trust.

The last part of our definition is incredibly important. Including the concept of decisional advantage allows CIP practitioners to build a business use case for trust network

validation and assessment activities. Several studies have touched upon the importance of trust in business decisions. For example, a 2019 article in *Management Science* conducted by students at MIT and UT-Dallas found several connections between supply chain decisions and trust networks (Choi et al., 2020). This is obvious on its surface: a CIP practitioner must trust the information upon which security decisions are made. This, in turn, will have significant financial and regulatory impacts. But the acquisition of trusted information via a validated trust network is hugely important. Decisions made with unverified or bad information will, without fail, yield bad outcomes.

The point of a trust network is to add trust to new pieces of information as quickly as possible while identifying what information is untrustworthy by using the elements of the network itself. The benefit is that a trust network can assign trust to the new information far more effectively than one CIP practitioner can through individual contacts with individuals from a cohesive trust network. For example, if telecommunications regional security managers routinely meet to discuss the latest security trends, they will likely learn from another regarding requirements and share information. Over time, they will build trust with one another. When one of the regional security managers obtains new information from a public-private partnership they are exclusively engaged with, they will introduce that piece of information into the network. The other regional security managers will then add trust to this new piece of information.

From this definition, it is also useful to adopt an inclusive view of CIP trust networks. CIP practitioners are inherently part of a trust network, whether they actively participate in it or not. For example, even in the most junior CIP practitioner role, say a night shift operator in a security operator center, the person filling that role has important information and positional authority which adds trust to pieces of information they share. If they were to call a local police department, for example, and alert the authorities to ongoing vandalism of fiberoptic cables, an additional level of trust would be assigned to their information.

The strength of a CIP practitioner's trust network is determined by their ability to assess and validate it, and whether they believe it is a valuable tool to achieve decisional advantage. Developing evidence-based and people-centric solutions to challenges and opportunities posed by AI will be a focus of proposed academic research moving forward.

Before moving forward with additional analysis, a brief literature review is offered to highlight the dearth of literature on CIP practitioner trust networks specifically, as well as the tangled web of regulations and compliance regimes in place to guide, and sometimes complicate, the work of CIP practitioners.

LITERATURE REVIEW

An exhaustive literature review of CIP practitioner trust networks finds little relevant information to assist the CIP practitioner in developing evidence-based and people-centric solutions to the problem of network validation. While there is a great deal of academic study on trust networks, and in the past 25 years since the attacks of 9/11, much has been written of the need for CIP practitioners to share information with each other and with every level of government, little research has been done concerning how these networks are assessed and validated, the efficacy of these assessments, and how trust networks are viewed within the CIP practitioner community.

By merging scholarly work on trust networks, with academic and governmental guidance on information sharing, we can begin to deduce evidence-based practices for CIP practitioners building trust networks. The merging of these concepts is important: cohesive networks do not add value to new information from interdisciplinary partners; information sharing by compliance regimes, or even public-private partnerships, could indicate a lack of trust. Only by discussing cohesion, the importance of weak ties, and information sharing do we approach a useful tool for CIP practitioners.

Trust Networks: Studies on Cohesion, Formal and Informal Roles Across Cultures

A large amount of academic literature has been published and peer-reviewed on the topics of trust networks; however, there is a dearth of studying trust networks amongst CIP practitioners. In addition to Wasserman and Faust, and Granovetter, mentioned above, dozens of researchers have studied trust networks. This robust set of literature is international and sociological in nature, ranging from studies of informal sharing networks like “blat” in Russia, or the concept of “guanxi” in China (Ledeneva, 2008) to studies of social trust in building markets in North Korea (Hastings & Yeo, 2024).

Because of the complexity of the topic, this literature review will focus on introducing concepts which will be discussed later in identifying evidence-based practices to assist CIP practitioners. Wasserman and Faust’s cohesive and affiliation network, Granovetter’s work on weak ties, have been built upon by others who discussed the levels of trust in a network. For example, Young Ae Kim, writing for the *Korea Advanced Institute of Science and Technology* in 2015, argued for a distinction between trust paths in homophily-based networks and expertise-based networks. Kim proposed that an increase in trust network density would improve trust propagation by increasing the number of trust paths between nodes (Kim, 2015).

Trust network research acknowledges important distinctions between formal and informal networks. This has an obvious corollary to CIP practitioners who navigate informal networks based upon personal networks and more formal networks such as public-private partnerships. It is important to note that formal and informal relationships have an impact upon trust and information sharing networks. Carmine Sellitto discussed this in a 2011 article for the *Journal of Interdisciplinary Social Studies* arguing:

> Formal organizational structures are typically documented and feature individual work units, departments, or operational areas. They can be easily identified, altered, downsized, or expanded to reflect the organization's direction and evolution. On the other hand, informal networks are relatively difficult to pinpoint and identify, even though they potentially underpin a firm's culture and constitution. Arguably, the formal organizational structure is very interdependent with the firm's informal networks, allowing the firm to function—be it in either a positive or negative manner (Sellitto, 2011).

This is an incredibly important concept for the CIP practitioner. The establishment of public-private partnerships combined with previously established homophily networks amongst CIP practitioners means that they must merge both formal and informal networks to achieve decisional advantage.

This short review reveals that no shortage of literature exists on the importance of the concept of trust in networks. Trust concepts span cultural boundaries and exist as a fundamental component of human existence. Despite this large body of literature on trust networks, no real emphasis has been placed on the complex task before CIP practitioners, namely, validating and weighing the impact of their trust networks.

Critical Infrastructure: Emphasis on Sharing, not Trust

Similarly to the amount of research done on trust networks, an immense body of academic and governmental research exists surrounding information sharing requirements surrounding critical infrastructure and CIP practitioners, but little research has been done concerning the developments of trust networks. There is, however, a great deal of guidance discussing the value of information sharing or information exchange amongst CIP practitioners. For example, President Biden's 2024 National Security Memorandum on Critical Infrastructure Security and Resilience stated the following:

> "The appropriate sharing of timely, actionable information, which may include relevant classified and unclassified intelligence and law enforcement sensitive information, among Federal, State, local, Tribal, and territorial entities; owners and operators; and other relevant stakeholders, is essential for effective risk management. The Federal Government will support a robust information sharing environment and public-private cooperation that enables actions and outcomes that reduce risk" (Biden, 2024).

Much of the emphasis on information sharing is specific to cybersecurity and cyber threat intelligence. Here, a common refrain goes, sharing intelligence is even more important because of the interconnected nature of the critical infrastructure landscape. The *National Institute of Standards and Technology (*NIST) 800-150 *Guide to Cyber Threat Information Sharing* is the gold standard that offers best practices in sharing information (National Institute of Standards and Technology [NIST], 2016). Some have

argued that an additional, global standard is required to govern cyber threat intelligence information. For example, in a 2025 article for the *Cyber Defense Review*, Diane Janosek argued, “Establishing a trusted global framework for cyber threat intelligence (CTI) sharing is essential to collective cyber resilience, deterrence, and defense. The lack of a global framework for CTI sharing hampers timely prevention of, and response to, cyberattacks. Governments, allies, and the private sector must collaborate across borders to establish secure, standardized, and legally compliant mechanisms for CTI exchange” (Janosek, 2025).

Cybersecurity protocols are incredibly robust and operate in areas of high regulation. Unsurprisingly, research amongst CIP cybersecurity practitioners is a bit more advanced than other disciplines of CIP. For example, Rick Randall and Stuart Allen wrote about cybersecurity information sharing sources and networks in 2021 in the *International Journal of Critical Infrastructure Protection*. Through an interview-based study, their work focused on how CIP practitioners validate their trusted sources and networks. Randall and Allen deduced that CIP practitioners assigned value to their trusted sources while also acknowledging networks of various degrees of closeness (Randall & Allen, 2021).

> “Three interviewees used a metaphor of “rings of trust” or “concentric circles of trust” in their comments to convey the concept that different degrees of trust consciously exist between different organizations, with corresponding differences in the types and frequency of content exchanged at each “ring”. Participants also mentioned how they rely on trusted sources from historical working relationships at current and previous organizations (e.g., when participants previously worked with or for law enforcement agencies)” (Randall & Allen, 2021).

While providing proof that CIP practitioners do assess and validate trust networks, Randall and Allen’s work does not provide evidence-based practices to support CIP practitioners.

This anecdotal evidence is helpful in understanding the informal nature in which CIP practitioners are likely to validate the information networks upon which they rely. It provides a useful framework for which to build evidence-based people-centric solutions.

Other researchers still focus on how information is shared amongst risk practitioners, including CIP practitioners. In a 2020 article for *Ecology and Society*, researchers in Australia found that when interdisciplinary teams “cocreate knowledge maps to help practitioners respond to disasters, preparedness is increased via the meshing of robust industry knowledge and evidence-based practices” (Barton et al., 2020). In other words, trust networks with interdisciplinary ties are crucial to developing CIP practitioner playbooks.

Stephen Corones and Bill Lane, in a 2015 article in Australia’s Deakin Law Review, tackled some of the legal ramifications of sharing critical infrastructure which might otherwise involve trade secrets. They argued that the sharing of information was so

critical that legislation may need to be introduced to facilitate the “frank exchange” of information (Corones & Lane, 2010). Acknowledging this trend, the US Government issued guidance, in 2016 and revised in 2020, in the Department of Homeland Security’s “Critical Infrastructure Information Sharing Framework.” This document sought to serve as:

> “…a resource to help critical infrastructure owners and operators, as well as other private sector, Federal, and State, local, tribal, and territorial (SLTT) government partners that share threat information, learn where they can turn, and in what circumstances, to both receive and report threat information. Threat information in this Framework is limited to information sharing pertaining to manmade threats, including both cyber and physical threats, to critical infrastructure (Cybersecurity and Infrastructure Security Agency” [CISA], 2016).

This document provided robust options for CIP practitioners to share information amongst each other and with the US government. These options include InfraGard, contacting a DHS fusion Center, or maintaining presence in a Homeland Security Information Network - Critical Infrastructure (HSIN-CI) channel.

The late 1990s saw a groundswell of support for critical infrastructure information sharing with InfraGard starting in 1996, and the establishment of Information Sharing and Analysis Centers (ISACs), authorized by Presidential order in 1998 (Clinton, 1998).

Membership in public-private partnerships like InfraGard may offer some CIP practitioners a venue where they may share information with trusted individuals. According to a 2024 press release from the FBI, “InfraGard is an FBI program that began in 1996 in the Cleveland field office as an effort to gain support from the information technology industry and academia for FBI investigations into threats against U.S. cyber infrastructure. After the events of September 11, 2001, the focus broadened to include cyber and physical threats to critical infrastructure and key resources” (Sekela & Shattuck, 2024). As noted above, membership in public-private partnerships may tend to bridge trusted information between networks and are therefore valuable for their ability to connect interdisciplinary teams. In this light, the information received by the organization itself may be less important than the information shared amongst members who would not otherwise be affiliated with one another.

Similar to InfraGard, ISACs have grown to become a valuable area for CIP practitioners to share information. Importantly, ISACs were established as public-private ventures and not regulators. In establishing the ISACs, President Clinton explicitly stated as much:

> “Since the targets of attacks on critical infrastructure would likely include both facilities in the economy and those in the government, the elimination of our potential vulnerability requires a closely coordinated effort of both the government and the private sector. To succeed, this partnership must be genuine, mutual, and cooperative in seeking to meet our national goal to eliminate the vulnerabilities of our

> critical infrastructure; therefore, we should, to the extent feasible, seek to avoid outcomes that increase government regulation or expand unfunded government mandates to the private sector" (Clinton, 1998).

Government, in an attempt to strike a balance between directing information sharing, avoiding undue regulation, and encouraging CIP practitioners to take matters into their own hands, has provided ample avenues to share CIP information. These venues bring with them the imprimatur of government support, but that does not necessarily equate to private sector adoption.

But the Federal Government has also mandated information sharing in other areas, such as data breaches. This is especially so in data breaches concerning HIPAA, FCC, FTC, or SEC regulations. Information sharing by compliance is different from a trust network where information flows in affinity networks. In fact, this is an important example of a lack of trust network: laws and regulations were instituted because information did not flow. This tacit acknowledgement of a breakdown in trust is an important topic upon which we will explore further below.

Thus, we have established that there is a great deal of research on trust networks and several government and industry-sponsored avenues for sharing valuable information. Government also mandates information sharing in certain instances.

Conclusion from Literature Review

From our review of literature concerning trust networks and information sharing amongst CIP practitioners, we find valuable lessons in the pursuit of evidenced-based people-centric solutions. First, ample research exists on the value of trust networks to support decision-making and accomplish common tasks. Second, incorporating weak ties as bridges can be a helpful force multiplier for cohesive and affiliation networks. Third, encouraging interdisciplinary teams may lead to more effective CIP solutions. Fourth, evidence exists that CIP practitioners do informally assess their networks and sources of trusted information. And fifth, the addition of regulation or compliance regimes, as well as governmental establishment of public-private ventures, simultaneously complicates and facilitates trust network development.

DISCUSSION AND ANALYSIS

Having defined trust networks, we will now turn to a discussion of some people-centric, evidence-based practices which CIP practitioners may use to validate, assess, and weigh the pros and cons of trust networks.

How do CIP practitioners assess and validate their own trust networks?

As indicated above, evidence exists that CIP practitioners actively assess and validate their trust networks through informal processes. This was highlighted most importantly through Randall and Allen's research in the *International Journal of Critical Infrastructure*. Although initially Randall and Allen did not seek out information concerning how trust networks are formed in the population they studied, they took note of several themes characterized by the following witness statements: "One of the requirements of our organization was to have trusted relationships in place," and further explained that "information sharing is a two-way street," meaning that both organizations in an information sharing arrangement have to perceive the relationship as having value to be effective over the long term (Randall & Allen, 2021). Two other interviewees, from different companies, explained that inter-organizational trust at their companies begins at an individual, interpersonal level and then develops over time to become more formally recognized at a company-to-company level" (Randall & Allen, 2021).

Thus, we see trust built over time from the bottom up as a crucial variable in how CIP practitioners generally assess and validate their trust networks. This informal way of building trust, however, does not account for the importance of weak ties, or the potential pitfalls of cohesive networks which can fragment over time.

This informal methodology also does not incorporate public-private partnerships, interdisciplinary and other important information sharing guidelines and regulations, discussed in our literature review.

Four Evidence-based, People and Organizational Assessment Methods and Tools

As described by Wasserman and Faust, as well as Barton et al., by detaching from one's informal trust network assessment frameworks, a more formal approach to trust network assessments may yield a more fulsome and useful assessment of one's CIP trust network.

1. Wasserman and Faust's affiliation matrix is a useful tool for practitioners to identify. This tool creates a two-mode matrix consisting of actors and organizations or events to determine where networks have strong and weak ties (Wasserman & Faust, 1994). A CIP practitioner can map their own network using their cohesive network, public-private partnerships organizations such as InfraGard or ISAC, any other organizations to which they belong, or events which they have attended, and adding in interdisciplinary partners as well as other CIP practitioners. From this

matrix, they can develop an evidence-based social network map of their CIP trust network that contains both cohesive ties and weak ties. This exercise may yield gaps in their network, or more likely, weak ties in interdisciplinary or organizational areas which can be relied upon to enhance decision-making.

2. Fortunately, the current social media landscape makes the construction of an affiliation matrix relatively easy. CIP practitioners can build and assess their networks on the professional networking website LinkedIn by using the 1st connection (strong) and 2nd, 3rd connections (weak) to learn more about their information networks. CIP practitioners can use those they deem most important in their trust networks and create a group for specific purposes. They can then use the 2nd and 3rd level connections to further assess the network for completeness between interdisciplinary levels. Finally, this exercise can identify key interdisciplinary partners with whom they should establish weak ties. CIP practitioners may test their networks by routinely asking questions (e.g., what is the most reliable weather application to use when preparing proactive response playbooks?) to see which weak ties are the most responsive.

3. CIP practitioners may further refine their trust networks by using the principles established herein and assigning variables to individuals and events/organizations in their networks. We have established that trust networks should be interdisciplinary in nature and not overly cohesive. A CIP practitioner should use temporal variables like length of relationships and frequency of contact to assess and drive interactions with a core group of individuals such as counterparts at similarly sized critical infrastructure facilities, their security teams, and local police departments. They may use role-based variables such as titles and functions to determine appropriate bridges between communities. Finally, they may use industry-adjacent variables such as enabling industries to further bridge or increase betweenness and information pathways. By employing a methodology to refine a trust network, CIP practitioners will likely receive more valid information and less useless information.

4. Finally, once a CIP practitioner has established their trust network, it is important to alert the bridges in the network of the type and quantity of information that is needed in order to achieve decisional advantage. This process of requirement generation and dissemination is an important aspect of CIP trust network implementation and validation. For example, if an energy sector CIP practitioner establishes a requirement to learn more information about potential criminal vandalism of sub-stations in neighboring counties, but they fail to learn about highly publicized incidents, they will learn that their trust network is not properly aligned to gather and add value to required information.

How effective are CIP practitioners in validating their trust networks and identifying gaps therein?

Given the gaps in methodologies for accurately assessing CIP trust networks, it is difficult to determine the efficacy of CIP practitioners' ability to validate those networks' utility. Efficacy regimes, however, can be grouped into several buckets: information sharing compliance, informal assessment, and Public-Private Partnerships participation. These regimes, however, do little to allow a CIP practitioner to validate their trust networks and mean that the ability of CIP practitioners to validate their networks is low. This further calls for additional methodologies to be incorporated into validation regimes.

Compliance Regimes:

In some cases, most notably, cybersecurity information sharing, compliance regimes have been established to mandate information sharing concerning critical infrastructure data breaches. As indicated below, these compliance regimes may actually indicate a lack of trust within a network, rather than a high degree of trust. Compliance rates, however, will not prove overly useful in validating a trust network. Moreover, the vast majority of critical infrastructure information sharing compliance regimes mandate sharing information following an incident. As we have proven, information sharing alone does not equate to a CIP trust network.

Informal Assessment Regimes:

As social animals, human beings in general and CIP practitioners specifically are inherently biased in making decisions. Their ability to assess their own trust networks is similarly biased in a number of ways, not the least of which is confirmation bias, mirror imaging bias, anchoring bias, and availability heuristics (Heuer, 1999). Yet, despite this, CIP practitioners are likely to assess their own trust networks via informal mechanisms as identified by Randall and Stuart. Relying upon contacts from previous employments in law enforcement or security, or memberships in public-private partnerships and professional organizations, CIP practitioners may assess their trust networks by feel, rather than process.

The problem with informal assessment regimes is that it ignores what we know to be true about trust network assessment. Namely, the importance of network density, weak ties, and trust propagation pathways between users.

Public-Private Partnership Regimes:

As discussed above, organizations like InfraGard and ISACs are great for bringing practitioners together to exchange data. These organizations allow for up-to-date information and immediately assign a modicum of trust to new pieces of information. A CIP practitioner, however, who solely relies upon these organizations may suffer from two of the danger areas discussed in this paper: overly cohesive networks and lack of interdisciplinary bridges. By valuing public-private partnerships appropriately, a CIP

practitioner can add them into a more robust network that incorporates information from partners in supportive industries or disciplines.

Evidence-Based Practices for Improving the Ability of CIP Practitioners to Assess Trust:

As it turns out, rotating through several levels of an organization may help yield better decision-making and ability to assess trust. By mandating that CIP practitioners rotate through various roles and levels of the CIP ecosystem, they will likely be able to independently decide which information, people, and organizations they may trust when making CIP decisions. Writing about supply chain decision-making in the journal *Management Science,* Choi and Zheng found the following:

> We show that, in addition, rotating managers across different functional roles and particularly engaging them in direct value chain functions during their career can help to train them on leveraging relevant knowledge to judiciously decide when and how much to trust in business interactions (Choi et al., 2020).

How do CIP Practitioners view the benefits and downsides of various trust networks, and does that impact their assessments?

CIP trust network creation and maintenance is both art and science. As we have shown, being able to assign trust to new information is a powerful concept and can lead to tangible benefits, most notably improved decision-making.

The downsides of trust networks are potentially dangerous. Bad information can still flow through vetted networks. In fact, bad information may flow quickly through a finely tuned trust network and yield to bad outcomes.

Moreover, poorly designed trust networks that are too cohesive and resistant to new information may actually stifle innovation and negatively impact security. For example, a security team may be tasked with monitoring criminal activity around fiber-optic cables nationwide. If that team only receives reports from the company's regional security managers, they will miss critical information from other information sources. A security team that has connections with local law enforcement, adequate tooling to ingest news and social media, relationships with other security teams as well as public-private partnerships and interdisciplinary partners will be better able to assign trust to new information and help the company achieve decisional advantage quickly.

Trust networks may also be susceptible to the same biases which impact the ability of CIP practitioners to assess and validate their own trust networks in the first place. This may be combatted by employing methodologies described herein (e.g., analyzing one's own trust network metrics). By focusing on bridging ties and incorporating an interdisciplinary approach to new information, it automatically applies a degree of vetting to new information. For example, if an energy infrastructure CIP practitioner has established bridges with multiple public-private partnerships, as well as other energy CIP practitioners regionally and globally, they may be able to obtain corroborating

information from several sources given a new potential threat vulnerability. Similarly, they may come across conflicting information which would need further vetting. Similarly, if the energy sector CIP practitioner builds their network with strong ties and bridges to interdisciplinary partners in cybersecurity, and HR/Talent functions, for example, they will be able to further vet information and add an additional layer of trust to new information.

Evidence-Based Practice to observe Positive and Negative effects of Trust Networks

The best way for CIP practitioners to objectively discern the good and the bad aspects of trust networks, as we have defined them, is to add evaluation of trust networks to their discussion items during robust after-action reviews (AARs) and tabletop exercises (TTXs). AARs following a significant event or exercise can assess the performance of a trust network. TTXs can identify weaknesses or gaps in a trust network. The following specific questions should be asked during these exercises to identify the trust network and if it is functioning in a positive or negative manner:

- Did the network provide accurate information?
- Did the network provide information useful to decisions?
- Did the network respond to requirements?
- Did the network incorporate new information and was this useful?

Conclusion

We close by restating our definition of a trust network:

> ***CIP Practitioner Trust Network Definition: A social network consisting of both formal and informal, strong and weak ties to facilitate bona fide information flow while also allowing new information and practices to enter the network, and complying with relevant regulations and laws, designed to achieve decisional advantage.***

This definition captures the complexity which faces CIP practitioners every day. By actively engaging in evidence-based practices to validate trust networks, practitioners will be able to more quickly assign trust levels to new information to make decisions. CIP practitioners are already engaging in informal assessments of their networks, but human cognition is plagued by biases which make this difficult. We have described several evidence-based practices to counter these biases and improve networks. Quicker and more accurate decisions lead to improved business cases for trust network development, which, in turn, leads to more robust investment in security. As we opened, we said, all CIP practitioners were inherently part of trust networks; your trust network will either feed you good information or bad information. A little bit of methodology goes a long way toward ensuring it's the former.

Author Biography

Mike Maloney is a strategic leader with over 25 years of experience in preparedness and crisis management. Mr. Maloney has served in positions in the United States Government and the private sector where he has provided enterprise-level risk consulting for global organizations.

Mr. Maloney holds an M.A. in Security Studies from Georgetown University's Walsh School of Foreign Service and a B.A. in Political Science from the University of Illinois at Urbana-Champaign.

Mr. Maloney's views expressed in this paper are his own and do not reflect the views of any current or former employer.

References

Barton, T. M., Beaven, S. J., Cradock-Henry, N. A., & Wilson, T. M. (2020). Knowledge sharing in interdisciplinary disaster risk management initiatives: Cocreation insights and experience from New Zealand. *Ecology and Society, 25*(4), 25.

Biden, J. R., Jr. (2024). National security memorandum on critical infrastructure security and resilience. *Daily Compilation of Presidential Documents*, 1–22.

Busby, J. W., Baker, K., Bazilian, M. D., Gilbert, A. Q., Grubert, E., Rai, V., Rhodes, J. D., Shidore, S., Smith, C. A., & Webber, M. E. (2021). Cascading risks: Understanding the 2021 winter blackout in Texas. *Energy Research & Social Science, 77*, 102106.

Choi, E. W., Özer, Ö., & Zheng, Y. (2020). Network trust and trust behaviors among executives in supply chain interactions. *Management Science, 66*(12), 5823–5849.

Clinton, W. J. (1998, May 22). *Presidential Decision Directive 63: Protecting America's critical infrastructures*. The White House.

Corones, S., & Lane, B. (2010). Shielding critical infrastructure information-sharing schemes from competition law. *Deakin Law Review, 15*(1), 1–36.

Cybersecurity and Infrastructure Security Agency. (2016, October). *Critical infrastructure threat information sharing framework*. U.S. Department of Homeland Security.https://www.cisa.gov/sites/default/files/publications/ci-threat-information-sharing-framework-508.pdf

Granovetter, M. S. (1973). The strength of weak ties. *American Journal of Sociology, 78*(6), 1360–1380.

Hastings, J., & Yeo, A. (2024). Markets and the development of social trust in the everyday politics of North Korea: Chinese entrepreneurs' perspectives. *Asian Studies Review, 48*(2), 313–330.

Heuer, R. J. (1999). *Psychology of intelligence analysis*. Center for the Study of Intelligence, Central Intelligence Agency.

Janosek, D. M. (2025). Toward a global framework for cyber threat intelligence sharing. *The Cyber Defense Review, 10*(2), 99–114.

Kim, Y. A. (2015). An enhanced trust propagation approach with expertise and homophily-based trust networks. *Knowledge-Based Systems, 82*, 20–28.

Ledeneva, A. (2008). 'Blat' and 'guanxi': Informal practices in Russia and China. *Comparative Studies in Society and History, 50*(1), 118–144.

National Institute of Standards and Technology. (2016). *Guide to cyber threat information sharing* (NIST Special Publication 800-150). U.S. Department of Commerce.

Randall, R. G., & Allen, S. (2021). Cybersecurity professionals' information sharing sources and networks in the U.S. electrical power industry. *International Journal of Critical Infrastructure Protection, 34*, 100454.

Sekela, A., & Shattuck, S. (2024). Joining InfraGard. *FBI Law Enforcement Bulletin*, 1–4.

Sellitto, C. (2011). Organisational structure: Some observations on the importance of informal advice and trust networks. *The International Journal of Interdisciplinary Social Sciences, 6*(2), 23–34.

Wasserman, S., & Faust, K. (1994). *Social network analysis: Methods and applications*. Cambridge University Press.

Wirth, L. (1938). Urbanism as a way of life. *American Journal of Sociology, 44*(1), 1–24.

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

Maloney, M. (2026). How CIP Practitioners Identify, Infer, and Validate Trust Networks:Using SNA to Identify Evidence-Based, People-Centric Best Practices. (Report No. 2026-1042). The Sam Houston State University. Institute for Homeland Security. https://doi.org/10.17605/OSF.IO/V843C

INSTITUTE FOR HOMELAND SECURITY
SAM HOUSTON STATE UNIVERSITY