ISSN: 2473-4901
v11 n6396

Social Networks and TTX Evaluation and Performance

Shawn F. Clouse
shawn.clouse@umontana.edu

Theresa Floyd
theresa.floyd@umontana.edu

College of Business
University of Montana
Missoula, MT 59812, USA

Ryan T. Wright
ryan.wright@virginia.edu
McIntire School of Commerce
University of Virginia
Charlottesville, VA 22904, USA

Patricia Akello
patricia.akello@mso.umt.edu

Reda Haddouch
reda.haddouch@umontana.edu

College of Business
University of Montana
Missoula, MT 59812, USA

Abstract

This study examines a multi-organization Tabletop Exercise (TTX) involving state and national agencies to provide insights into how social cognition and network factors influence exercise outcomes. Building upon Social Cognitive Theory and Social Network Theory, this study proposes a model that links psychological factors like self-efficacy and communication network structures to participants' perceptions of organizational performance and training benefits. The research explores how communication networks and people's confidence in their organization's abilities affect how participants view the exercise's success. The study highlights the importance of security self-efficacy, demonstrating how beliefs in organizational capability influence engagement and perceived success. By connecting psychological readiness with network structures, this work advances a more comprehensive understanding of how to design, implement, and evaluate impactful cybersecurity TTXs, ultimately strengthening preparedness for complex, high-stakes cyber incidents. Findings underscore the critical role of communication structures: participants embedded in larger and more central networks reported higher assessments of their organization's performance and the exercise's value. Additionally, perceived security self-efficacy emerged as a significant driver of positive outcomes. Practically, these results recommend structuring TTX for cohorts that may have differing maturity levels and facilitating broad and inclusive communication.

Keywords: Social networks, Cybersecurity tabletop exercises (TTXs), Critical infrastructure, Incident response.

ISSN: 2473-4901
v11 n6396

Social Networks and TTX Evaluation and Performance

Shawn F. Clouse, Theresa Floyd, Ryan T. Wright, Patricia Akello, and Reda Haddouch

1. INTRODUCTION

Cybersecurity professionals and government agencies have warned that the US power grid and critical infrastructure are vulnerable to devastating malicious attacks (Ling, 2025). As cyber threats to critical infrastructure continue to rise, organizations across both public and private sectors are turning to Tabletop Exercises (TTXs) as a key tool for cybersecurity and incident response preparedness. For example, "Operation 999" was a ransomware TTX focused on the water industry, which allowed participants an immersive experience to practice incident response strategies (Leyden, 2025). TTXs offer a low-cost, scenario-based method to simulate incident response and test decision-making, coordination, and communication strategies in a safe, controlled environment. They combine experiential learning with realistic scenarios to train organizational personnel effectively (Maurer, 2023). When implemented, these exercises significantly enhance both technical and essential soft skills, bridging gaps frequently observed among professionals and new graduates (Angafor et al., 2020). These exercises are especially valuable for improving not only technical readiness but also soft skills such as collaboration, leadership, and adaptability (Angafor et al., 2020; Pate et al., 2016).

Empirical evidence from healthcare, education, transportation, and the pharmacy sectors reinforces the effectiveness of TTXs, showing substantial improvements in knowledge, attitudes, confidence, and practical response capabilities compared to traditional lecture-based training (Brunner & Lewis, 2006; Mirzaei et al., 2020; Pate et al., 2016; Radow, 2007). Businesses frequently rely on TTX for their cybersecurity training and preparedness needs (Pearlson et al., 2021). Further, CISA, the U.S. government organization charged with protecting national cybersecurity and infrastructure from cyber threats, actively endorses this training method by providing ready-made TTX packages, reflecting their advocacy as a standard practice (*Cybersecurity & Infrastructure Security Agency*, 2025). Moreover, the National Institute for Standards and Technology (NIST) has put TTX as a common and valuable practice in their NIST Cybersecurity Framework (CSF) to help organizations test and improve their response capabilities (National Institute of Standards and Technology, 2024). In summary, Tabletop exercises (TTXs) are widely used for emergency preparedness by several disciplines, including Cybersecurity, and much work has gone into the design of these programs, yet effective Cybersecurity TTX implementation is not as well understood (Haddouch et al., 2024). Despite widespread use, the effectiveness of TTXs is not well understood; this study addresses that gap by examining how social cognition and network structure shape outcomes.

The goal of TTX is to assess an organization's preparedness and response capabilities for various scenarios by simulating real-world situations in a low-risk, discussion-based environment (Cybersecurity & Infrastructure Security Agency, 2025). A key outcome is developing and testing coordination and communication (Everbridge, 2025; Haddouch et al., 2024). In a literature review, Vykopal et al. identified 140 research papers explicitly examining TTXs. "Out of only three papers (P4, P6, and P8) that addressed assessment, only one (P6) suggested a method that goes further than unstructured assessment by the observers and facilitators" (Vykopal et al., 2024, p. 223). There is an opportunity to provide a theoretically driven, rigorous assessment of the outcomes of the TTX beyond observational data.

This study focuses on evaluating participants' perceptions of their organization's performance and the benefits gained from a TTX situated in the context of critical infrastructure protection in rural areas, where resource constraints and unique communication challenges make effective team coordination and training implementation particularly important. This research examines the impact of a key learning factor drawn from social cognitive theory (Bandura, 1997), in concert with factors related to the network of interactions between participants to better understand how to effectively implement and evaluate TTXs in cybersecurity and beyond. This research identifies key psychological and contextual factors—such as self-efficacy (belief in one's ability to accomplish a specific task), network size, and network centrality (one's structural position within a network)—that are often overlooked in traditional linear TTX evaluations. Thus, this study supports the

ISSN: 2473-4901
v11 n6396

development of a research model that explains how these factors shape perceived performance and benefits during TTXs, particularly in resource-constrained environments like rural infrastructure settings. By connecting psychological readiness and social networks, this research offers a more comprehensive understanding of how to implement and evaluate impactful TTXs in cybersecurity and beyond.

2. LITERATURE REVIEW & THEORETICAL FOUNDATION

Tabletop exercises: Design, efficacy, and evaluation gaps

Tabletop exercises (TTXs) are increasingly used across critical infrastructure sectors to simulate cyber threats in controlled, non-disruptive environments. Additionally, TTXs have emerged as an effective method for enabling participants to collaboratively address complex cybersecurity incidents affecting critical infrastructure. According to Evans (2019), such scenarios provide a low-stress yet high-impact setting that enables participants to enhance their comprehension of cyber threats while improving their collaborative, communicative, and decision-making abilities in simulated real-world conditions (Evans, 2019). In complex scenarios, the integration of public-private partnerships and civilian-military collaboration becomes essential.

As Elvegård and Andreassen (2024) emphasize, TTXs facilitate interagency coordination by engaging multiple organizations, thereby enhancing mutual recognition of cyber risks and increasing awareness of shared resources and response capabilities (Elvegård & Andreassen, 2024). Maennel et al. (2023) stress the necessity of joint efforts across sectors to develop comprehensive cyber-defense mechanisms capable of addressing large-scale, multifaceted security incidents. The inclusion of diverse disciplinary perspectives and varying levels of expertise within these exercises further enriches the collective problem-solving process.

A critical element of interagency collaboration is establishing a clear understanding of roles and shared expectations during cybersecurity incidents. In alignment with these principles, the NIST 800-84 guidelines (Grance et al., 2006) endorse TTXs as a key component within broader test, training, and exercise (TT&E) programs aimed at strengthening preparedness for cybersecurity events. Organizations should adopt best practices for TTXs to be prepared to address security events.

Bartnes and Moe (2017) identify several critical success factors in the design and execution of TTXs, including clearly defined objectives, time-sensitive decision points, realistic role assignments, and active involvement of key stakeholders. When these elements are met, TTXs have the potential to enhance both technical competencies and non-technical skills, such as leadership and collaboration (White et al., 2004; Young & Farshadkhah, 2022). Despite their recognized value, much of the existing literature primarily assesses TTXs through the lens of compliance and organizational readiness benchmarks. Less attention has been paid to the interpersonal and structural dynamics that shape the efficacy of these exercises.

Tobergte et al. (2022) argue that the most impactful TTXs are those that replicate authentic cognitive and emotional stressors, mirroring the uncertainty and complexity of real-world incidents. Nonetheless, empirical investigations into interactional patterns—such as communication flows, centrality in problem-solving networks, and their influence on learning outcomes remains limited. The current study seeks to fill this gap by examining the relational and organizational conditions that optimize learning and coordination in cybersecurity tabletop exercises.

Social Cognitive Theory

Social Cognitive Theory (SCT) posits that individuals' beliefs about their capabilities influence their behavior, motivation, and outcomes (Bandura, 1977, 1997). When extended to the group or organizational level, collective efficacy reflects the shared belief that the team or organization is capable of successfully performing a given task. In the cybersecurity context, this theoretical lens has proven powerful in explaining behavioral variation in both proactive and reactive security behaviors.

A landmark early application of this theory in the information systems domain is found in Compeau and Higgins (1995). In the study, Compeau and Higgins (1995) developed and validated a scale for computer self-efficacy (CSE) and demonstrated its predictive power for individual computer usage behavior, beyond actual skill level. CSE was updated in 2022 to IT self-efficacy (ITSE) as CSE has a narrow desktop-centric view of computing, which does not translate to the platform and mobile environment of today. ITSE acknowledges that confidence in using IT now extends to environments where users may interact with systems indirectly (e.g., voice interfaces, AI tools) or rely on highly automated systems (D. Compeau et al., 2022). Extending

ISSN: 2473-4901
v11 n6396

this to the cybersecurity domain, Johnston and Warkentin (2010) applied self-efficacy theory to model end-user compliance with security policies. The study empirically tested the role of self-efficacy alongside fear-based appeals in shaping users' security behavior intentions, finding that users who believed in their ability to enact secure behaviors were significantly more likely to avoid risky actions such as opening phishing emails or using weak passwords (Johnston & Warkentin, 2010). Further, Stavrou and Piki (2024) found that cultivating self-efficacy is a key attribute in developing cybersecurity skills. These findings highlight the importance of psychological readiness in shaping security-related performance.

Similarly, Ifinedo (2012) used social cognitive theory to explore employee compliance intentions within organizations. The study advanced a model that integrates self-efficacy within a broader behavioral framework, combining the Theory of Planned Behavior (TPB) and Protection Motivation Theory (PMT) to examine what drives user compliance with security policies. His findings demonstrate that self-efficacy, perceived behavioral control, and response efficacy are key predictors of intention to comply with security policies. This work is particularly relevant in organizational contexts where employee awareness, confidence, and perceived capability significantly influence security posture (Ifinedo, 2012). In the context of cyber team readiness, Durcikova et al. (2024) empirically examined how organizational cybersecurity self-efficacy relates to real-world breach outcomes, reinforcing the view that collective belief systems or organizational security self-efficacy are predictive of performance in high-uncertainty, high-stakes environments like cybersecurity (Durcikova et al., 2024). In sum, there is clear evidence that social cognition plays an important role in technology interactions and decision making, which are both critical in TTXs.

Social Network Theory

While social cognitive theory explains why individuals and teams may engage in effective behavior during TTXs, Social Network Theory helps explain how those behaviors unfold across communication structures. Social Network Theory conceptualizes social systems as sets of nodes (people) and ties (interactions), and emphasizes how structural position within a network affects access to resources, influence, and information (Borgatti & Li, 2009; Burt, 1992; Freeman, 1978). Two constructs—network size and centrality—are relevant in time-sensitive, collaborative environments like TTXs. In an early application of social network theory to organizational behavior, Brass (1984a) conducted a study on organizational influence, revealing that individuals with high centrality in communication networks wield significant informal power, often surpassing those with formal authority. The study found that structural position within a network, i.e., centrality, is an important predictor of influence over decision-making and performance outcomes (Brass, 1984). This principle was extended to emergency management and security contexts by Monge & Contractor (2003), who extended Social Network Theory into high-pressure organizational environments, demonstrating that communication structure, not just technical expertise, plays a decisive role in determining team effectiveness during complex coordination tasks. Their work underscores the predictive value of network properties such as density and connectivity for group performance (Monge & Contractor, 2003).

In the cybersecurity space, Gordon et al. (2003) argued for the importance of inter-organizational information sharing in preventing security breaches and proposed early models of collaborative security readiness. The authors emphasized that timely and strategic information flow between networked actors is essential for preempting and mitigating security breaches, shifting the focus from isolated technical controls to collaborative readiness (Gordon et al., 2003).

A study examining cybersecurity skills, specifically phishing detection within organizations, found that an individual's centrality within a department, as determined by social network analysis, is associated with cybersecurity compliance (Wright et al., 2023). In addition, this study found that IT self-efficacy was identified as another factor related to cybersecurity skills and compliance. Similarly, Carley (2003, 2020) introduced the concept of social cybersecurity, applying computational network analysis to assess how information spreads through human networks and how trust and influence can be compromised. Her work highlights the importance of modeling not just who participates in exercises, but who connects, influences, and facilitates coordination; ideas that this study seeks to test in an applied TTX setting (Carley, 2003, 2020). Individual interactions and relationships, as assessed by a social analytics lens, are interconnected in significant situations and can influence outcomes. The authors believe this may be true in TTX as well.

Research hypotheses

Building upon Social Cognitive Theory and Social Network Theory, this study advances a

theoretically grounded model to explain how perceived organizational security efficacy and communication network structure may influence participants' perceptions of organizational performance and training benefit in cybersecurity Tabletop Exercises (TTXs). The hypotheses center around psychological antecedents (self-efficacy), structural mediators (network position), and the exercise-level outcomes (perceived performance and benefit).

Perceived security self-efficacy

Grounded in Social Cognitive Theory, perceived self-efficacy in the context of TTX refers to an individual's belief in their team or organization's ability to effectively respond to cyber threats. This belief serves as a motivational driver, influencing how participants approach engagement with team members and respond to simulated stress scenarios during the exercise.

Past research has long established the positive influence of self-efficacy across various domains (Bandura, 1997; Staples et al., 1999). At the team level, cybersecurity-specific self-efficacy reflects the collective confidence of a group in executing cyber incident response tasks (Judge & Bono, 2001). Recent empirical work also reinforces this view. Durcikova et al. (2024) investigated how collective self-efficacy within cybersecurity teams affects an organization's resilience against breaches . The study found that high team efficacy led to fewer and less severe security incidents, emphasizing that belief in competence influences not just individual behavior but also organizational vigilance and cohesion. Similarly, Park and Shin (2022) applied social cognitive theory to explore how group-level efficacy shaped team coordination during security-critical tasks, finding that overconfidence can sometimes degrade performance unless coupled with strong communication and accountability mechanisms. These findings align with the broader theoretical expectation that groups with elevated levels of self-efficacy and trust in their organization tend to exhibit better performance outcomes (Park & Shin, 2022; Ter Huurne & Gutteling, 2009).

These psychological factors are not only critical for performance but also shape interpersonal dynamics during TTXs. Specifically, higher levels of self-efficacy may lead participants to contribute more actively to group dialogue, express concerns, and initiate communication more freely. These behaviors, in turn, influence the structure and quality of in-exercise communication networks, including participants' connectedness and central roles within those networks.

Within the TTX environment, this research posits that heightened perceived security self-efficacy enables teams to more efficiently access and disseminate critical information, facilitating quicker and more effective connections to relevant actors and knowledge. Therefore:

H1: Perceived organizational security *self-efficacy is positively related to in-exercise communication network (a) size and (b) centrality.*

In-exercise communication networks

While individual-level beliefs serve as behavioral antecedents, the structure of communication during a TTX also plays an important role in shaping outcomes. Drawing from Social Network Theory (Borgatti et al., 2009; Freeman, 1978), this study examines two network-level constructs: a) network size and b) network centrality. These metrics capture the relational architecture of a TTX and are central to understanding how influence, coordination, and information flow unfold in real time.

The social network perspective conceives of the interconnected relationships and interactions between individuals as an informal structure that provides opportunities and imposes constraints (Borgatti et al., 2009). By examining the informal structure of the participants' communication during the exercise, the researchers explore how the relational context influences participants' access to information, ability to share information, and their influence on others, thus providing a deeper understanding of the factors affecting their perceptions of their organization's performance and the benefits of the exercise.

Network size is defined by the number of people each participant identified as effective communicators during the exercise (Freeman, 1978). Larger networks are associated with greater access to information and resources (Borgatti et al., 2009). Network centrality can be defined in several different ways. This study used *closeness network centralit*y (Freeman, 1978; Valente & Foreman, 1998), which is defined by the number of links it takes for each participant to reach all the other participants through the network. This concept of centrality is associated with independent access to information (because one has many potential contacts from which to gather information) and through this access, increased influence over others (Brass, 1984). Accordingly, in organizational crisis response, actors who are more central or better connected are often more influential in steering team decisions and synthesizing intelligence (Brilingaitė et al., 2022).

ISSN: 2473-4901
v11 n6396

Therefore, the study expects that participants whose in-exercise communication networks are larger and whose positions within the networks are more central will evaluate their organization's performance in the exercise more favorably and will more highly rate the benefits of the exercise to their organization.

H2: In-exercise communication network size is positively related to a) perceived organizational performance in the TTX and b) perceived benefits of the TTX.

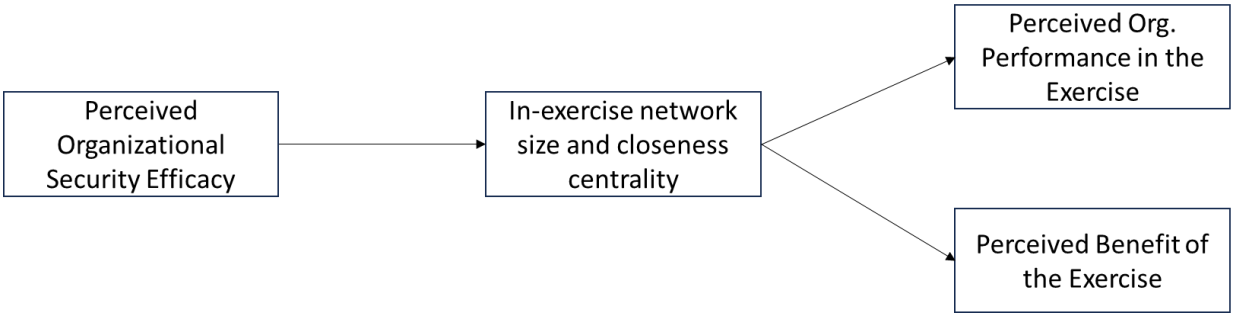
H3: In-exercise communication network centrality is positively related to a) perceived performance in the TTX and b) perceived benefits of the TTX.

Further, this research expects that in the high information velocity context of the TTX, where access to and control of information is highly important, a participant's network size and centrality will mediate the relationship between self-efficacy and the outcomes.

H4: In-exercise communication network size will mediate the relationship between perceived organizational security efficacy and a) perceived organizational performance and b) perceived benefits of the TTX.

H5: In-exercise communication network centrality will mediate the relationship between perceived organizational security efficacy and a) perceived organizational performance and b) perceived benefits of the TTX.

Figure 1. Integrated Model Based on Social Cognitive Theory and Social Network Theory.



Research model

The above hypotheses are depicted in the conceptual model shown in Figure 1. The model integrates psychological beliefs (self-efficacy), communication structure (network size and centrality), and perceived outcomes (performance and benefit), providing a theory-driven explanation for variability in TTX effectiveness. In the proposed model, participants with higher perceptions of organizational security efficacy will have larger in-exercise communication networks and will be more central in those networks. In turn, in-exercise network size and centrality will influence participants' perceptions of their organizations' performance in the exercise and the benefits of the exercise for their organizations. Additionally, this research expects that in certain high-information velocity environments (e.g., TTX), where access to and control of information is highly important, the properties of a participant's in-exercise communication network (e.g., size and centrality) will mediate the relationship between self-efficacy and the outcomes.

3. METHODS

Study setting and TTX description

The study was situated in the context of critical infrastructure protection in rural areas, where resource constraints and unique communication challenges make effective team coordination and training implementation particularly important. The TTX was conducted in a rural state in the Rocky Mountain West within the electrical industry.

The TTX session started with an interdisciplinary planning team that organized the event and developed the exercise. The planning team included staff from the state's flagship university, staff from the Cybersecurity and Infrastructure Security Agency (CISA), staff from the state conducting the TTX training, and members from the critical infrastructure organizations. The planning team met several months prior to the event to develop goals for the TTX, develop the participant list, design the scenario for the exercise, and devise a plan to identify gaps during the after-action review. This exercise used the

ISSN: 2473-4901
v11 n6396

DECIDE Platform from Norwich University Applied Research Institutes (*NUARI*, n.d.) as a decision support system to be used during the exercise. DECIDE was developed with funding from the Department of Homeland Security, and it has been a trusted cybersecurity live exercise solution. The platform simulates cyber-attacks for organizations and their partners to stress and test incident response plans, resulting in after-action reports to improve strategic communication, compliance, risk, and overall resilience. The platform launches the different stages of the scenario in an email inbox interface. Participants can respond via a chat tool and there is a survey tool to capture qualitative and quantitative responses for each step of the TTX.

This exercise was designed to practice coordination, communication, and information sharing protocols between electric grid partner organizations while responding to a hypothetical disruptive cyber and physical incident. The integration of government, industry, military, and academia provides a strategic opportunity to work toward informed state-wide solutions with a robust network of partners. The participants in the exercise included employees from the public power company, 20 energy cooperatives, the Electric Cooperatives' Association, the state fusion center, the state Cybersecurity and Infrastructure Security Agency (CISA) representatives, National Guard, and state IT.

Procedure and participants

The event was held for six hours in two adjoining rooms at a large northwestern university. There were 25 players from the power industry and 21 players from state and federal agencies as well as the National Guard. Most of the participants (43) attended in person, and three attended virtually via an internet video conferencing system (Zoom). All participants used laptops that were connected to the NUARI DECIDE Platform. All players, observers/scribes, and facilitators received DECIDE training prior to the TTX. NUARI provided staff to troubleshoot problems and to advance the injections for the exercise. The exercise scenario is described in Appendix 1. The in-person participants were assigned to eight groups distributed between two rooms at the facility; virtual participants were assigned to a ninth group. Each group included managers and technical staff from a power company or cooperative, as well as a National Guard representative.

There were facilitators for each step of the exercise as well as a facilitator for the virtual group. The facilitators roamed around to make sure each group was making progress on the discussion. There were 26 scribes who took notes on the discussions of the nine groups over the four modules of the TTX. The scribes all signed a Non-Disclosure Agreement, agreeing to keep the names of the participants and the organizations confidential. Their notes were submitted on the DECIDE Platform as a chat message. The facilitators introduced each step of the scenario, and the participant teams were given 20 minutes for discussion. Then everyone was brought back together for a 15-minute large group discussion following each step of the TTX. During the 20-minute team discussions, few players entered comments into the DECIDE platform, so the content of the discussion was primarily captured by the scribes in DECIDE. The large group discussion was broadcast between the two rooms of the facility and to the virtual participants via Zoom. Prior to launching the next stage of the exercise, participants were given five minutes to respond to open-ended and Likert questions on the DECIDE Platform.

Survey instruments, measures, and analysis

Online surveys were distributed via the DECIDE platform as well as via Qualtrics survey software (Qualtrics, Provo, UT). DECIDE was used to deliver questions that were asked as part of the tabletop exercise. Qualtrics was used for the two surveys in the research design: a pre-test survey before the exercise to elicit participants' organizational security efficacy, organization information, and demographics, and a post-test survey after the exercise to elicit participants' in-exercise networks, and ratings of their organization's performance during the exercise and benefits of the exercise for their organization. Both survey invitations were emailed to participants. The pre-test survey took about 10 minutes, and the post-test about 20 minutes. The data collected on Qualtrics, was stored on a separate protected server, which only the researchers had access to. The Qualtrics surveys were encrypted using SSL security.

Respondents were assigned a random ID code by the survey software. The investigators maintained one roster file containing participants' names and ID codes. This roster file was password protected and only accessed by the researchers. All analysis was done with the random ID code to protect the identity of the participants. The network map about who interacted with whom during the exercise is non-sensitive data that the organizations will use only to aid in future incident response planning. All participants were entered into a drawing for gift cards that were given out at the end of the TTX event. Participants could complete the survey

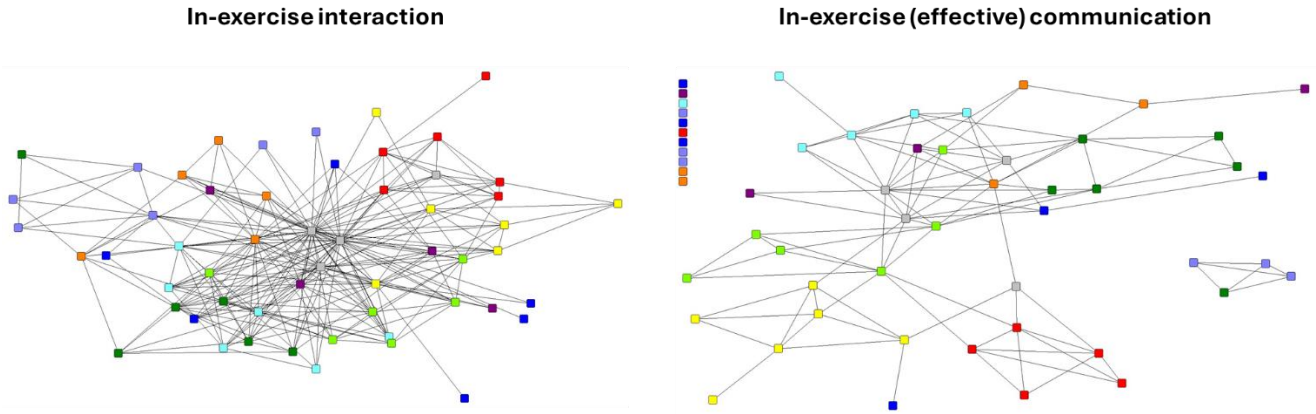
ISSN: 2473-4901
v11 n6396

only once, so incentives did not influence participation beyond survey completion.

Outcome and social cognitive variables were measured using Likert-type scales where 1= strongly disagree and 7= strongly agree. A complete list of survey items and confirmatory factor analyses is shown in Appendix 2. *Perceived organizational performance* in the exercise was measured using a 6-item scale adapted from Park & Shin (2022) and (Cammann et al., 1979). Sample item: "Our organization exceeded its objectives for dealing with this cyber incident." *Perceived benefit of the exercise* was measured using a 3-item scale developed by (Wu & Wang, 2006) Sample item: "The tabletop exercise will benefit my organization." *Perceived organizational security efficacy* was measured using a three-item scale developed by Park & Shin (2022). Sample item: "My organization has above-average ability in responding to cybersecurity events."

The in-exercise communication network was elicited using a one-item measure, in which participants were asked to view a roster of all participants and check the box next to the names of anyone "who was especially effective at communicating during the exercise" (Marsden, 1990). The resulting network was symmetrized using the maximum method, so that if either member of a pair named the other as an effective communication partner, the tie counted (Borgatti et al., 2024). Network variables were calculated using UCINET VI (Borgatti et al., 2002). *Network size* was calculated using degree, a count of the number of people in each participant's communication network (Freeman et al., 1987). *Network closeness centrality* was calculated using

Figure 2. In-exercise Interaction and Communication Networks.



Average Reciprocal Distance (ARD) (Valente & Foreman, 1998), which averages the reversed geodesic distance between an individual and all others in the network, thus indicating the extent to which each participant had access to many effective communicators during the exercise.

This study tested several potential control variables, including age, race, gender, organizational affiliation, rank, position tenure, veteran status, organization size, number of employees in the organization's cyber unit, and number of cyber breaches. Only organization size and number of cybersecurity employees were significantly related to the outcome variables, so all other controls were deleted for the sake of parsimony. Frequencies for categorical control variables are available in Appendix 3.

4. RESULTS

Refer to Figure 1 for the theoretical model, which outlines the hypothesized relationships between organization security self-efficacy, in-exercise communication network size and centrality, and perceived performance during the exercise and the benefit of the exercise. The sample size is insufficient for structural equation modeling (Wolf et al., 2013); thus, the authors used ordinary least squares (OLS) regression

analyses to test for direct relationships and the PROCESS macro (Hayes, 2012) in IBM SPSS Statistics (version 29) for the path analysis of the mediation model. Indirect effects were tested using 5,000 bias-corrected bootstrap samples (Preacher & Hayes, 2008).

Network maps

Figure 2 presents the map of the in-exercise interaction and communication networks. Nodes are colored according to group membership, with gray nodes indicating facilitators. Recall that the communication network identifies especially effective communication ties, so the

ISSN: 2473-4901
v11 n6396

communication network is sparser than the general interaction network.

Descriptives and zero-order correlations

Table 1 presents descriptive statistics and zero-order correlations. The relatively high means for perceived organization performance (5.52 out of 7) and benefit of the exercise (6.14 out of 7) indicate that participants generally thought their organizations had performed well and saw value in the exercise. Pre-exercise perceptions of organizational security efficacy were also relatively high (5.21 out of 7), indicating that participants generally believed that their organizations were competent to deal with cybersecurity incidents.

Table 1. Descriptive Statistics and Zero-order Correlations.

Variable	*N*	*Mean*	*SD*	*Min*	*Max*	1	2	3	4	5	6
1 Perceived organizational performance	39	5.52	0.87	3.00	7.00						
2 Perceived benefit of the exercise	39	6.14	0.83	4.00	7.00	.57**					
3 Perceived organizational security efficacy	43	5.21	1.61	2.00	7.00	0.29	-0.10				
4 In-exercise communication network size	55	3.67	2.98	0.00	13.00	.43**	0.32	0.22			
5 In-exercise communication network centrality	55	12.47	7.73	0.00	24.00	.33*	0.27	.33*	.83**		
6 Number of cyber professionals in organization	39	94.10	359.35	0.00	2000.00	-0.31	-0.29	0.30	0.25	0.16	
7 Number of employees in organization	39	1019.44	2806.18	8.00	17000.00	0.05	-.45**	0.11	0.15	0.12	0.46

Note. Table presents bivariate correlations. N=39
* $p < .05$. ** $p < .01$.

Model testing

Results of OLS regression analysis predicting perceived organizational performance in the exercise are presented in Table 2, that show the relative influence of organizational security efficacy and network factors on performance. Communication network size and centrality were entered separately in Models 3 and 4 to effectively test the effects of each variable because social network variables, while theoretically distinct, are often empirically correlated.

The number of cybersecurity professionals in the organization was consistently negatively related to evaluations of performance, while perceived organizational security efficacy was consistently positively related. Both network variables were positively related to performance evaluations, with network size demonstrating a larger effect size. There is some evidence for a mediation effect, since with the addition of both network variables to the model, the effect size and significance of perceived organizational security efficacy was reduced.

Results of OLS regression analysis predicting perceived benefit of the exercise are presented in Table 3. This time, the significant control variable is organization size (number of employees), which remains significantly related to perceived benefit in every model. Perceived organizational security efficacy is negative, though not significantly, related to the perceived benefit. Both network variables are positively related to the outcome, with network size having a slightly larger effect size. Since perceived organizational security efficacy is not significantly related to perceived benefit, there is no evidence suggesting mediation.

ISSN: 2473-4901
v11 n6396

Table 2. Results of OLS Regression Analysis Predicting Perceived Organizational Performance in Tabletop Exercise.

	Model 1	Model 2	Model 3	Model 4
	β *(SE)*	β *(SE)*	β *(SE)*	β *(SE)*
Number of cybersecurity professionals in organization	-.31† (.00)	-.43* (.00)	-.53*** (.00)	-.48** (.00)
Perceived organizational security efficacy		.36* (.08)	.27† (.07)	.26 (.08)
In-exercise communication network size			.53*** (.04)	
In-exercise communication network centrality				.35* (.02)
Model F	3.79†	4.69*	9.94***	5.30**
R2	0.10	0.22	0.48	0.33
Change in R2		0.12	0.26	0.11
Adjusted R2	0.07	0.17	0.43	0.26

$N = 39$. † $p < .10$ * $p < .05$ ** $p < .01$ *** $p < .001$.

Table 3. Results of OLS Regression Analysis Predicting Perceived Benefit of Tabletop Exercise.

	Model 1	Model 2	Model 3	Model 4
	β *(SE)*	β *(SE)*	β *(SE)*	β *(SE)*
Number of employees in organization	-.45** (00)	-43** (.00)	-.48** (.00)	-.46** (.00)
Perceived organizational security efficacy		-.11 (.08)	-.21 (.07)	-.24 (.08)
In-exercise communication network size			.44** (.04)	
In-exercise communication network centrality				.40* (.02)
Model F	8.65**	4.55*	7.13***	5.99**
R2	0.20	0.21	0.39	0.35
Change in R2		0.01	0.18	0.14
Adjusted R2	0.18	0.17	0.34	0.29

$N = 39$. † $p < .10$ * $p < .05$ ** $p < .01$ *** $p < .001$.

Table 4. Simple Mediation PROCESS Models Examining the Effect of Organizational Security Efficacy on Organizational Performance Through In-Exercise Communication Network Size and Centrality.

	Model 1 Mediating variable Network size	Model 2 Mediating variable Network centrality	Model 3 Dependent variable Perceived Performance	Model 3 Dependent variable Perceived Performance
	β *(SE)*	β *(SE)*	β *(SE)*	β *(SE)*
Independent variables				
Number of cybersecurity professionals in organization	.00 (.00)	.00 (.00)	-.00*** (.00)	-.00** (.03)
Perceived organizational security efficacy	.30 (.30)	1.15† (.68)	.14† (.07)	.14* (.08)
Mediator variables				
In-exercise communication network size			.16*** (.04)	
In-exercise communication network centrality				.14 (.08)
Mediation (indirect effests)			Effect [95% CI]	Effect [95% CI]
Security efficacy ->Network size ->Performance			.05 [-.04, .13]	
Security efficacy ->Network centrality ->Performance				.05 [-.01, .17]
Constant	3.00† (1.58)	8.76* (3.52)	4.10*** (.38)	4.17*** (.45)
F- statistic	1.62	2.46	9.94***	5.30**
R^2	0.09	0.13	0.47	0.33

Note. $N = 37$. All mediation tests were done using 5,000 bootstrap samples.
* $p < .05$ ** $p < .01$ *** $p < .001$.

ISSN: 2473-4901
v11 n6396

Table 4 summarizes mediation tests, showing that while efficacy predicts performance, network size and centrality operate as independent predictors rather than mediators. Models 1 and 2 indicate that perceived organizational security efficacy is not significantly related to either network size or centrality. Moreover, tests of indirect effects indicate that neither of the mediations are supported. These results demonstrate that communication network size and centrality are independent predictors of the two outcomes, rather than mediators between the outcomes and perceived security efficacy. These results suggest that while perceived organizational security efficacy was positively related to performance, it was not associated with perceived benefit of the exercise. One possible explanation is that participants who already had strong confidence in their organization's security capability viewed the exercise as less beneficial, since they perceived limited new value to be gained. This contrasts with the consistent positive effects of communication network variables, which appear to shape both performance perceptions and perceived benefit.

5. DISCUSSION

This study contributes to the research on the effective implementation of TTX by examining the effects of factors drawn from social cognitive theory and social network theory on TTX outcomes. Few studies have examined how the "human element" affects TTX outcomes or focused on collecting data to evaluate the effectiveness of TTX implementation; thus, this research moves beyond the typical linear format to better explicate what combination of factors enhance performance and benefits in a TTX exercise, providing a more comprehensive understanding of how to implement and evaluate TTXs going forward.

Theoretical and practical implications

First, it is important to point out that the participants in general were highly engaged and perceived great benefits from the TTX exercise (mean = 6.14/7). This indicates they generally saw value, which is a necessary condition for tabletop exercises to be successful (Pearlson et al., 2021). That said**,** this research also found that employees of larger organizations with more cybersecurity professionals evaluated their organization's performance and the benefit of the exercise less favorably. This may indicate that organizations with advanced cybersecurity protocols may derive less value from TTXs in their current format. It might be useful for practitioners to consider creating different exercises for different cohorts based on the level of cybersecurity maturity, although it is likely that participants from smaller organizations likely benefited greatly from their interactions with the participants from larger organizations. Further research could seek to tease apart the overlapping benefits for different groups.

Second, this research found that perceived security efficacy, a key social cognitive factor, is significantly associated with participants' perceptions of their organization's performance during the exercise but is not associated with their perceived benefit of the exercise. Perhaps higher confidence in their organization's security efficacy contributed to participants' effectiveness during the exercise, although an alternative explanation could be that their confidence painted a rosy picture of their performance and may have contributed to less critical attention to certain aspects of the event. Future research could augment the collection of participants' perceptions of performance with objective performance measures to compare the two. It is also interesting that enhanced confidence led participants to negatively evaluate the benefits their organizations could gain from the exercise (although the relationship was not statistically significant). Participants who view their organization as already competent often see limited value in current TTXs. This supports the first findings about perceived benefits and corroborates the suggestion that more advanced exercises may be preferable. Grouping organizations by cybersecurity maturity and security self-efficacy could also be effective.

Third, this study found that both network variables had larger effect sizes than perceived security efficacy in predicting the outcome variables, suggesting that in-exercise communication, and the access to information and influence that it provides, is an important factor to be examined further. This study also found that communication network size was a stronger predictor of both outcomes than communication network centrality, suggesting that the simpler measure might be an effective factor to consider, greatly simplifying data collection and analysis for practitioners who want to take social networks into account. Facilitators need to actively engage organizations to involve their entire network within the TTX (and probably a real cyber response) for the best outcomes.

Finally, this research learned that social cognitive and social network factors were independently related to perceived performance, with no support indicating the mediation relationship hypothesized. Future research could dig deeper to

ISSN: 2473-4901
v11 n6396

examine other psychological readiness constructs as potential antecedents to in-exercise interaction and cooperation, which would help researchers and practitioners better prepare participants for TTXs, perhaps leading to enhanced outcomes.

Limitations and future research

The small size of this sample means that the results should be interpreted with caution and that future research should attempt to replicate these results in different contexts, since there is likely a good bit of difference in TTX implementation and evaluation in different industries and geographical locations. Future research could also triangulate participants' perceptions with objective performance data to validate whether overconfidence influences exercise evaluations. Additionally, although the pre-post research design allowed the authors to make reasonable assumptions about causality, future researchers could further examine the relationships uncovered using a longitudinal design, perhaps evaluating how former participation in TTXs affects performance in later TTXs and actual cyber events.

6. CONCLUSION

This study had an opportunity to study a multi-organization TTX that included state and national agencies. The goal of this research was to provide novel insights into how social cognition and network factors influence the outcomes of a TTX. This study contributes to the emerging literature in TTX as these findings underscore the significant role of communication networks, specifically network size and centrality. This research also highlights the importance of security self-efficacy for performance outcomes. Practically, these results recommend structuring TTX for cohorts that may have differing maturity levels and facilitating broad and inclusive communication.

7. REFERENCES

Angafor, G. N., Yevseyeva, I., & He, Y. (2020). Game-based learning: A review of tabletop exercises for cybersecurity incident response training. *Security and Privacy*, *3*(6), e126. https://doi.org/10.1002/spy2.126

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191. https://psycnet.apa.org/journals/rev/84/2/191/

Bandura, A. (1997). *Self-efficacy: The exercise of control*. Macmillan. https://books.google.com/books?hl=en&lr=&id=eJ-PN9g_o-EC&oi=fnd&pg=PA116&dq=Bandura,+A.+(1997).+Self-Efficacy:+The+Exercise+of+Control.&ots=zAKQJZl91k&sig=G7Ptkv_fG-if4lLQORFi2kIhlQI

Bartnes, M., & Moe, N. B. (2017). Challenges in IT security preparedness exercises: A case study. *Computers & Security*, *67*, 280–290. https://doi.org/10.1016/j.cose.2016.11.017

Borgatti, S. P., Agneessens, F., Johnson, J. C., & Everett, M. G. (2024). *Analyzing Social Networks*. https://www.torrossa.com/gs/resourceProxy?an=5730558&publisher=FZ7200

Borgatti, S. P., Everett, M. G., & Freeman, L. C. (2002). *Ucinet 6 for Windows: Software for social network analysis*. ResearchGate. https://www.researchgate.net/publication/216636663_UCINET_for_Windows_Software_for_social_network_analysis

Borgatti, S. P., & Li, X. (2009). On social network analysis in a supply chain context. *Journal of Supply Chain Management*, *45*(2), 5–23.

Borgatti, S. P., Mehra, A., Brass, D. J., & Labianca, G. (2009). Network Analysis in the Social Sciences. *Science*, *323*(5916), 892–895. https://doi.org/10.1126/science.1165821

Brass, D. J. (1984). Being in the Right Place: A Structural Analysis of Individual Influence in an Organization. *Administrative Science Quarterly*, *29*(4), 518. https://doi.org/10.2307/2392937

Brilingaitė, A., Bukauskas, L., Juozapavičius, A., & Kutka, E. (2022). Overcoming information-sharing challenges in cyber defence exercises. *Journal of Cybersecurity*, *8*(1), tyac001. https://doi.org/10.1093/cybsec/tyac001

Brunner, J., & Lewis, D. (2006, December). Tabletop Exercises Can Train All the Staff for Safety. *The Education Digest*, *72*(4), 46–49. https://www.proquest.com/docview/218186889/abstract/FDEFEB4F2CD04258PQ/1

ISSN: 2473-4901
v11 n6396

Burt, R. S. (1992). *Structural Holes: The Social Structure of Competition* (SSRN Scholarly Paper 1496205). Social Science Research Network. https://papers.ssrn.com/abstract=1496205

Cammann, C., Fichman, M., Jenkins, D., & Klesh, J. (1979). The Michigan organizational Assessment Questionnaire. *Unpublished Manuscript, University of Michigan, Ann Arbor*.

Carley, K. M. (2003). *Dynamic Network Analysis*.

Carley, K. M. (2020). Social cybersecurity: An emerging science. *Computational and Mathematical Organization Theory*, *26*(4), 365–381. https://doi.org/10.1007/s10588-020-09322-9

Compeau, D., Correia, J., & Thatcher, J. (2022). When Constructs Become Obsolete: A Systematic Approach to Evaluating and Updating Constructs for Information Systems Research. *Management Information Systems Quarterly*, *46*(2), 679–712. https://aisel.aisnet.org/misq/vol46/iss2/5

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly*, *19*(2), 189. https://www.proquest.com/docview/218139743/abstract/96833716E0B04773PQ/1

Cybersecurity *& Infrastructure Security Agency*. (2025). CISA Tabletop Exercise Packages | CISA. https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

Durcikova, A., Miranda, S. M., Jensen, M. L., & Wright, R. T. (2024). United We Stand, Divided We Fall: An Autogenic Perspective on Empowering Cybersecurity in Organizations. *MIS Quarterly*, *48*(4), 1503–1536. https://doi.org/10.25300/misq/2024/17211

Elvegård, R., & Andreassen, N. (2024). Exercise design for interagency collaboration training: The case of maritime nuclear emergency management tabletop exercises. *Journal of Contingencies and Crisis Management*, *32*(1), e12517. https://doi.org/10.1111/1468-5973.12517

Evans, C. A. (2019). Tabletop exercises in the nursing classroom: An introduction for nurse educators. *Nursing Forum*, *54*(4), 669–674. https://doi.org/10.1111/nuf.12394

Everbridge. (2025, April 9). What is a Tabletop Exercise? *Everbridge*. https://www.everbridge.com/blog/conducting-effective-tabletop-exercises-for-emergency-preparedness/

Freeman, L. C. (1978). Centrality in social networks conceptual clarification. *Social Networks*, *1*(3), 215–239. https://doi.org/10.1016/0378-8733(78)90021-7

Freeman, L. C., Romney, A. K., & Freeman, S. C. (1987). Cognitive Structure and Informant Accuracy. *American Anthropologist*, *89*(2), 310–325. https://doi.org/10.1525/aa.1987.89.2.02a00020

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy*, *22*(6), 461–485. https://doi.org/10.1016/j.jaccpubpol.2003.09.001

Grance, T., Nolan, T., Burke, K., Dudley, R., White, G., & Good, T. (2006). Guide to test, training, and exercise programs for IT plans and capabilities. *NIST*. https://www.nist.gov/publications/guide-test-training-and-exercise-programs-it-plans-and-capabilities

Haddouch, R., Clouse, S. F., Wright, R. T., Floyd, T., & Perry, P. (2024). *Strengthening Incident Response: Lessons from Cybersecurity Tabletop Exercises for Rural Critical Infrastructure*.

Hayes, A. F. (2012). *PROCESS: A versatile computational tool for observed variable mediation, moderation, and conditional process modeling*. University of Kansas, KS. https://www.researchgate.net/profile/Ludmil

ISSN: 2473-4901
v11 n6396

a-Zajac-Lamparska/post/How-can-I-analyze-baseline-measures-as-predictors-of-change-in-longitudinal-designs/attachment/59d61de779197b807797c2a0/AS%3A273843497701387%401442300786437/download/Hayes+process.pdf

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, *34*(3), 549–566. https://doi.org/10.2307/25750691

Judge, T. A., & Bono, J. E. (2001). Relationship of core self-evaluations traits—self-esteem, generalized self-efficacy, locus of control, and emotional stability—with job satisfaction and job performance: A meta-analysis. *Journal of Applied Psychology*, *86*(1), 80–92. https://doi.org/10.1037/0021-9010.86.1.80

Leyden, J. (2025, June 17). *Operation 999: Ransomware tabletop tests cyber execs' response | CSO Online*. https://www.csoonline.com/article/4006349/operation-999-ransomware-tabletop-tests-cyber-execs-response.html

Ling, J. (2025, June 2). The US Grid Attack Looming on the Horizon. *Wired*. https://www.wired.com/story/youre-not-ready-for-a-grid-attack/

Maennel, K., Brilingaitė, A., Bukauskas, L., Juozapavičius, A., Knox, B. J., Lugo, R. G., Maennel, O., Majore, G., & Sütterlin, S. (2023). A Multidimensional Cyber Defense Exercise: Emphasis on Emotional, Social, and Cognitive Aspects. *SAGE Open*, *13*(1), 21582440231156367. https://doi.org/10.1177/21582440231156367

Marsden, P. V. (1990). Network Data and Measurement. *Annual Review of Sociology*, *16*(1), 435–463.

Maurer, T. (2023, September 18). 6 Actions CEOs Must Take During a Cyberattack. *Harvard Business Review*. https://hbr.org/2023/09/6-actions-ceos-must-take-during-a-cyberattack

Mirzaei, S., Eftekhari, A., Sadeghian, M. R., Kazemi, S., & Nadjarzadeh, A. (2020). The Effect of Disaster Management Training Program on Knowledge, Attitude, and Practice of Hospital Staffs in Natural Disasters. *Journal of Disaster and Emergency Research*, *2*(1), 9–16. https://jder.ssu.ac.ir/article_48.html

Monge, P. R., & Contractor, N. (2003). *Theories of Communication Networks*. Oxford University Press. https://doi.org/10.1093/oso/9780195160369.001.0001

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29; p. NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

NUARI*: Addressing National Cyber Security Issues*. (n.d.). Retrieved September 7, 2024, from https://nuari.org

Park, H., & Shin, S. (2022). When Does Group Efficacy Deteriorate Group Performance? Implications of Group Competency. *Behavioral Sciences*, *12*(10), 379. https://doi.org/10.3390/bs12100379

Pate, A., Bratberg, J. P., Robertson, C., & Smith, G. (2016). Evaluation of a Tabletop Emergency Preparedness Exercise for Pharmacy Students. *American Journal of Pharmaceutical Education*, *80*(3), 50. https://doi.org/10.5688/ajpe80350

Pearlson, K., Thorson, B., Madnick, S., & Coden, M. (2021). Cyberattacks are inevitable. Is your company prepared? *Cybersecurity and Digital Privacy, Harvard Business Review*. https://cams.mit.edu/wp-content/uploads/2021-03-09-v3-LIVE-HBR-Cyberattacks-Are-Inevitable.-Is-Your-Company-Prepared1.pdf

ISSN: 2473-4901
v11 n6396

Preacher, K. J., & Hayes, A. F. (2008). Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. *Behavior Research Methods*, *40*(3), 879–891. https://doi.org/10.3758/BRM.40.3.879

Radow, L. J. (2007). *Tabletop exercise guidelines for planned events and unplanned incidents/emergencies*. https://trid.trb.org/View/1152626

Staples, D. S., Hulland, J. S., & Higgins, C. A. (1999). A Self-Efficacy Theory Explanation for the Management of Remote Workers in Virtual Organizations. *Organization Science*, *10*(6), 758–776. https://doi.org/10.1287/orsc.10.6.758

Stavrou, E., & Piki, A. (2024). Cultivating self-efficacy to empower professionals' re-up skilling in cybersecurity. *Information & Computer Security*, *32*(4), 523–541.

Ter Huurne, E. F. J., & Gutteling, J. M. (2009). How to trust? The importance of self-efficacy and social trust in public responses to industrial risks. *Journal of Risk Research*, *12*(6), 809–824. https://doi.org/10.1080/13669870902726091

Tobergte, P., Landsberg, L., & Knispel, A. (2022). *Evaluation of Tabletop Exercises in Emergency Response Research and Application in the Research Project SORTIE*.

Valente, T. W., & Foreman, R. K. (1998). Integration and radiality: Measuring the extent of an individual's connectedness and reachability in a network. *Social Networks*, *20*(1), 89–105. https://doi.org/10.1016/S0378-8733(97)00007-5

Vykopal, J., Čeleda, P., Švábenský, V., Hofbauer, M., & Horák, M. (2024). Research and Practice of Delivering Tabletop Exercises. *Proceedings of the 2024 on Innovation and Technology in Computer Science Education V. 1*, 220–226. https://doi.org/10.1145/3649217.3653642

White, G. B., Dietrich, G., & Goles, T. (2004). Cyber security exercises: Testing an organization's ability to prevent, detect, and respond to cyber security events. *Proceedings of the 37th Annual Hawaii International Conference on System Sciences.* https://doi.org/10.1109/HICSS.2004.1265411

Wolf, E. J., Harrington, K. M., Clark, S. L., & Miller, M. W. (2013). Sample Size Requirements for Structural Equation Models: An Evaluation of Power, Bias, and Solution Propriety. *Educational and Psychological Measurement*, *73*(6), 913–934. https://doi.org/10.1177/0013164413495237

Wright, R. T., Johnson, S. L., & Kitchens, B. (2023). Phishing Susceptibility in Context: A Multilevel Information Processing Perspective on Deception Detection. *MIS Quarterly*, *47*(2).

Wu, J.-H., & Wang, Y.-M. (2006). Measuring KMS success: A respecification of the DeLone and McLean's model. *Information & Management*, *43*(6), 728–739. https://doi.org/10.1016/j.im.2006.05.002

Young, J., & Farshadkhah, S. (2022). Teaching Cybersecurity Incident Response Using the Backdoors & Breaches Tabletop Exercise Game. *Cybersecurity Pedagogy & Practice Journal*. http://www.cppj.info/2022-1/n1/CPPJv1n1.pdf

Appendix

Appendix 1. TTX Exercise.

Electrical Grid TTX1 Modules and Questions

Event Purpose: The United States will continue to face critical risk to its critical infrastructure from state, non-state actors and criminal networks. The state as a rural state continues to be at risk from limited resources and critical national investment in protecting critical infrastructure. As part of the nation's critical infrastructure, 3 sectors stand out as critical to national functions: electricity, telecommunications, and finance. Known as the tri-sector; they hold most of the critical national functions critical to state functions. This exercise is designed to be the start of a series of cyber incident response exercises to discover gaps, vulnerabilities and most importantly solutions to cross sector and cross function incident response. The integration of government, industry, military, and academia provides a strategic opportunity to work toward informed state-wide solutions with a robust network of partners.

Participants: Public Energy Utility (electrical generation, transmission, and distribution), twenty electric distribution cooperatives, National Guard, State fusion center, Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA), and a state university.

Scenario: Tensions continue to rise in globally as China threatens Taiwan for strong returns in their most recent Presidential election for a candidate that emphasized a free and independent Taiwan and elimination of the one China policy. China in turn has ramped up mobilization of PLA and PLN resources forecasting a lethal response or invasion to repulse an independent Taiwan recognized by global powers. China has also ramped up greater cyber intrusions on US national infrastructure, interested in strategic US military facilities for force projection, nuclear response, and mobilization. These intrusions are focused on US military systems, defense industrial base systems and critical components of the electric grid supporting military installations and outlying Strategic Command facilities.

Exercise Objectives:

- Identify key relationships in an escalatory cyber incident in an electric distribution scenario.
- Identify key organizational capability gaps in responding to an escalatory cyber incident (local/State/federal)
  - Training and education gaps
  - Authorities and policy gaps
  - Response capabilities and capacity
  - Process and relationships
- Identify the key processes for cross organizational escalatory cyber incident
- Identify key questions and decisions required at private-public interface (local/state)
- Identify what resources are available from the federal government (specific organizations) to enhance state, local government, and industry

Training Objectives for Organizations

Industry Partners:

- Identify key decisions and processes required in an escalatory cyber incident
- Develop relationships and mature processes to respond to an escalatory cyber incident
- Develop basic gaps analysis for organizational response plan
- Identification of war stoppers, policy and authority issues with partner (local/state/federal)
- Identify resource requirements to enhance incident response planning and exercising
- Identify outside resources available and the process for requesting support during a cyber incident

State Government

- Identify key decisions and processes required in an escalatory cyber incident
- Develop relationships and mature processes to respond to an escalatory cyber incident
- Develop basic gaps analysis for state response plan
- Identification of war stoppers, policy and authority issues with partner (local/state/federal)

- Identify resource requirements to enhance incident response planning and exercising
- Identify outside (Federal) resources available and process to request for cyber incident

National Guard

- Identify and describe National Guard capabilities available to the state for cyber event
- Identify authorities, policy gaps to respond to state cyber incident and interaction with private industry (what can they do and what are they capable of doing)
- Identify reporting requirements and the approval process for cyber incident response (e.g., the 9-line program)
- Identify capability and capacity gaps for state response to cyber incident response

University

- Identify opportunities to support gaps analysis and requirements development
- Identify opportunities for university leadership
- Identify opportunities for workforce professional development (future workforce and professional development of current workforce)

Deliverables:

- Student-Observer, Researcher and DECIDE questions data
- After action report on key objectives above
- Researcher whitepaper on Identified gaps from exercise
- Proposals (Roadmap) for series of exercises (annual/semi-annual or quarterly)
- Gaps analysis report (internal with partners)

Tabletop Scenario

Module 1

Day 1 – Wednesday April 19th

Your industrial control system (ICS) software provider recommends a new critical security update for its industrial control systems in the upcoming weeks. The patch is downloaded by a staff engineer's laptop and then uploaded to your system's Programmable Logic Controller(s) (PLC).

Discussion Questions

1. What is the greatest cyber threat to your organization? To the energy sector?
2. What processes are in place to vet third-party vendors and their patches (software authenticity & integrity checks)
3. Describe the security controls in place for the engineer's laptop.
4. How are personnel who update ICS systems vetted and trained?

Day 2 – Thursday April 20th

The Cybersecurity Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) released a joint alert regarding a phishing campaign targeting energy companies over the past three months. A suspected global hacker group has been observed discussing on dark web forums a sophisticated phishing strategy to cast a wide net to attack as many energy sector businesses and ICS systems as possible.

Your organization also receives information from other cyber intelligence sources that report incidents of threatening notes and emails being delivered, information on a widespread phishing campaign against a bank, and known malicious actor groups.

Day 6 – Monday April 24th

All Electricity Information Sharing and Analysis Center (E-ISAC) members receive an email alert from "alerts@Energy-ISAC.co". The alert warns members regarding threats to the electrical grid via a watering hole on websites frequented by organization employees. The alert is quickly identified as a spoof by E-ISAC, and you are notified via E-ISAC Portal Notification "noreply@mail.eisac.com" of its untrustworthiness. CISA and FBI amplify E-ISAC's Portal Notification for situational awareness.

Discussion Questions

1. What actions would you take based on the alerts in this scenario?
2. What cybersecurity threat intelligence do you currently receive?

   a. What cybersecurity threat intelligence is most useful?
   b. How is the information shared internally?
   c. How do you assess intelligence to determine its relevance?
   d. When you receive a significant number of alerts/reports from many different sources, what process is used to identify the most important/actionable information?
3. With different types of intelligence (physical vs cyber, electric sector vs general cyber activity, local vs national/global), how does your organization balance these different intelligence topics/sources?
4. What factors are considered for you to determine an intelligence source to be trustworthy?
5. Given the false information received in the above incident, what factors would you consider for attempting to validate any other intelligence you receive?
   a. What internal/external partners would you contact to validate these sources?
   b. How would you contact trustworthy intelligence sources?
6. What alternative methods can intelligence be shared if normal channels are compromised or potentially untrustworthy?

Day 7 – Tuesday April 25th

A spear-phishing email is received by your operators of the transmission system from a typo-squatting energy provider account. The email asks the target to change their credentials that access the Market Portal. Some in your organization report the email to their management or security officer; others complete the request to change passwords/credentials.

Discussion Questions

1. Describe your organization's cybersecurity awareness training program.
2. What topics does the training address?
   a. How often are personnel required to complete the training?
   b. Are simulated phishing emails included in the training?
   c. What are the consequences for not completing training?
   d. How do you track and enforce cybersecurity awareness training?
3. How do employees report possible phishing emails?
   a. What actions are taken after a phishing email is reported?
4. How/What is the process in place you would use to share this intel with other organizations?
5. Because it appears as though the energy provider has been potentially compromised, how would you handle validating the energy provider's communications?
6. What communication/expectation would you have from the energy provider in addressing this issue?
7. What alternative communications/reporting methods are available?

Module 2

Day 8 – Wednesday April 26th

Breakers begin opening and closing on electric equipment on the grid. The alternating breakers are becoming erratic enough to cause intermittent outages. An investigation is opened to discover the root cause of the breaker issues.

Discussion Questions:

1. At what point would you notify law enforcement, regulators, or others in government of these incidents?
   a. What are the thresholds for requesting external assistance?
2. What resources would you need to manage these incidents?
   a. What resources are immediately available?
   b. What outside partners, if any, would you contact for assistance or advice?
3. How are you communicating with your operations teams that are trying to stabilize the grid?

Day 10 – Friday April 28th

Residents and business owners begin calling customer service and your operations center regarding the outages. Some customers report that the intermittent power issue is tripping their emergency generators.

Day 13 – Monday May 1st

Throughout the night, affected residents take to social media sites, including your company's online platforms, to complain about the lack of power, claiming their calls to the operations center and customer service are being ignored.

As workers continue to troubleshoot around the clock, for every load reenergized, another indicator alerts to a power loss. More customers call in to report outages.

Your customer service and your operations center receive calls from local healthcare providers regarding continued outages and letting the operations center know of failures in their local backup generator.

Discussion Questions

1. Who is authorized to represent the company on social media? To the news network media?
2. How would you manage interactions with the media or the public?
3. What are employees supposed to do if they are contacted by media?
4. How do you share information internally?
5. Do you provide media training to team members to react to these incidents?
6. As these events play out, who do you share information with?
    a. What information do you share? Who does the sharing?
    b. How do the Electrical Coop Association members support each other?
    c. How does the Electrical Coop Association and the public utility support each other?
7. Could any of the events described in this module be classified as cybersecurity incidents? If so, how should they be handled?
8. At what point would you refer to your cybersecurity incident response plan?
    a. How would you handle this incident per the plan?
    b. How are your cyber/physical plans coordinated during incident response?

Day 15 – Wednesday May 3rd

Local police receive multiple reports of individuals taking photographs of transmission lines, transformers, and electric substations. Although no suspects were questioned to date, some reports indicate that the individual may have been dressed in a uniform resembling those local utility workers wear and may have had a backpack containing tools. Concurrently, other electric cooperatives observed some suspicious activity at a few of its electric substations.

Recently, the Federal Bureau of Investigation (FBI) released a Joint Intelligence Bulletin (JIB) warning of possible sabotage to telephone lines, specifically those relating to 911 services. In response to the JIB, the Electricity Information Sharing and Analysis Center (E-ISAC) issued an industry advisory concerning the need for increased vigilance and reporting of suspicious activity.

Discussion Questions

1. Has state Electric Cooperative Association members and the public power company identified to law enforcement the level of importance of regional and local critical infrastructure (e.g., electric substation, communications, and electrical vaults)?
2. What security or intruder detection measures are employed at both above ground and underground communication vaults? At local electric substations?
3. If your organization received information related to "suspicious behavior" or potential threats against your facilities and personnel, how would you communicate this information to appropriate industry partners or authorities?
    a. What are your local reporting procedures (e.g., local suspicious activity reporting [SAR]), and which entities would you notify?
    b. Is your organization aware of the Nationwide SAR Initiative?
    c. Is your organization familiar with how to contact your local law enforcement, Joint Terrorism Task Force (JTTF), state fusion center, FBI Office, and local CISA Protective Security Advisor (PSA)?
4. What measures might you ask of local law enforcement at this time to protect your organization and / or facilities (e.g., outreach, increased vigilance)?

5. What internal information sharing and dissemination processes does your organization currently use?
    a. How does your organization triage the information it receives (e.g., formal reporting, rumors, social media) for further dissemination within the organization and to personnel?
    b. Are nationwide trends of suspicious behaviors within your industry and across the Energy Sector tracked locally?
    c. Who is responsible for coordinating the risk communications message for your organization?
    d. How would implementation of protective measures be communicated?
    e. Are there technological barriers, legal considerations, or institutional sensitivities that might affect information sharing or prohibit use of electronic communication during specific times?
6. Given current and established information sharing procedures, what types of official information are the most useful (immediate information versus analyzed information) to your organization?
    a. Does your organization use the Homeland Security Information Network – Critical Infrastructure – Electricity (HSIN-CI - Electricity) portal?
    b. Does your office habitually receive E-ISAC Industry Advisories or JIBs that are pertinent to your organization?
    c. Does your organization receive security threats or protective measure information from trade organizations, manufacturers, consultants, or other industry partners?
    d. Does your organization perform independent analysis on information provided? If so, describe the process?

Module 3

Day 20 – Monday May 8th

Grid Operations Center crews notice the turbine over rev is exceeding recommended operational revolutions per minute. Two issues develop: electrical output is increased beyond the level transformers can handle, and the turbine starts to fail from the heat generated along its power shaft. As the turbine spins out of control, crews attempt to conduct an emergency shutdown. However, they are unable to completely de-energize the system before the transformers fail. This creates a cascading effect across the grid as it attempts to keep up the demand for electricity.

Day 21 – Tuesday May 9th

As state energy companies attempt to recover from the cyber incident, it is discovered that replacement turbine parts are delayed 6-12 months due to supply chain issues.

Discussion Questions

1. How do you manage crews (Field or Operation Center Crews) across days of repairing energy grids?
2. How are systems/grids prioritized for recovery efforts?
    a. How do you determine the criticality of each system/grid?
    b. How is this defined by your business continuity and recovery plans?
    c. What backup systems can be deployed?
        i. How quickly can they be deployed?
        ii. How are they verified and updated?
3. How do you share resources among other electric sector members in the event of a major grid issue?
4. How are field crews communicating back to respective Controls Rooms to provide updates/assessments on the state of grid equipment?
5. How do grid failures impact the stability/energy flows across the greater state Interconnection?
    a. What type of communication is happening with other regions in the state?
6. How does this impact the running of other parts of the business (such as the Markets)?
7. What information would you share with the media?
8. How does the delays in replacement parts impact grid recovery and reliability?
9. Given the new timeline on repairing equipment (6-12 months out) how does this impact the running of other parts of the business (such as the Markets)

Day 22 – Wednesday May 10th

After a thorough investigation, it was discovered that the malfunctioning grid and transformers were a result of a patch containing malware that infected industrial control systems (ICS).

Day 23 – Thursday May 11th

Several media outlets contact your organization seeking comments about the increasing power outages. Local new stations around the state report of healthcare providers, small businesses, schools, and government facilities are struggling with providing services due to the increasing power outages. The report states that businesses that have backup generation have not properly tested their backup equipment and they are not working properly.

Discussion Questions

1. What is your change management process to determine if any other update/upgrade could also be contributing?
2. How do you determine if a recent software patch has adversely affected your systems?
3. What processes and resources are in place for cyber evidence preservation and forensics?
    a. At this point what information are you sharing with external partners (particularly those participating in this exercise)
4. How are you balancing decisions around executing your cybersecurity incident response plans to contain & eradicate while also keeping the grid running?
5. What level of risk are you willing to accept to keep the electric grid running when you have software/equipment that has been compromised?
6. If you find that other organizations are also victims of these incidents, what factors are considered for sharing incident information? What value is there in sharing? What channels/capabilities do you have for open sharing incident information?
7. What outside partners, if any, would you contact for assistance or advice
8. For the State and Federal partners in the room, at this point how can you be of assistance?
9. How do you determine if an attacker is in or still in your system?
10. How do you monitor suspicious or anomalous network activity for IT systems?
11. How do you recover your Industrial Control Systems?
12. IT Backups vs OT Backups. Are they the same? Where are the backups stored? Are they offline or online, stored in a secure location, or managed by a third party?
    a. Are backups tested to ensure they work and are not corrupted, infected, or damaged?
    b. How far back can your backups recover?
    c. How often is the data restoration process exercised?
13. What information would you share with the media?
    a. Would you share any information about the malware with the media?

Module 4

Day 25 – Saturday May 13th

Residents experience disruptions in attempts to place and receive 911 calls using their landline telephones. Citizens that were unable to place landline calls successfully used mobile telecommunications to notify 911 operators and their telephone service providers of the problem.

The location of the communications disruption is determined to be near an electric substation. Local Co-op workers are dispatched to the site and begin surveying to determine the locality and cause of the disruption.

Law enforcement officers are dispatched to a local electric substation after receiving reports of sporadic gunfire being directed at the substation. Meanwhile, the local electric utility company facility operators notice system abnormalities and begin implementing safety protocols. After a cursory search around the perimeter of the substation facility, police officers discover several "large metal boxes" leaking fluid, possibly oil.

Upon analysis, state's Analysis and Technical Information Center which is the state's Fusion Center determines that this closely resembles an event outlined in an E-ISAC Portal Notification from Day 15 – May 3rd. When this information is forwarded to the local FBI Field Office, they issue a JIB for release to local law enforcement and the private sector, stating that this is a recurring method of sabotage.

Discussion Questions

1. Would the electric utility company be notified by the telecommunications company of the communications disruption or vice versa of any power disruption?
    a. Would the 911 dispatch office contact either the electric company or telecommunication company to report any disruption of service or inquire about the duration for repair?
    b. Should there be more sharing of real-time information between telecommunication and electric substation entities, particularly when interruption of communications may be an initial sign of an attack?
2. Are first responders (e.g., law enforcement, fire fighters, and emergency services) aware of any specific concerns or hazards associated with responding to incidents at electric substations?
3. Do your organization's emergency response plans (e.g., site security plans, emergency evacuation plans, emergency action plans, or other appropriate plans) contain protocol for properly responding to incidents described in this module?
    a. How often does your organization review its emergency response plans, and does it perform drills to test their effectiveness?
    b. Do your organization's response plans address how to coordinate power restoration priorities?
    c. Do your organization's response plans account for law enforcement evidence-gathering requirements?
    d. Have cross-sector dependencies been incorporated into your organization's response plans?
    e. Have resulting impacts or cascading effects on other electricity components within the Energy Sector been incorporated into your organization's response plans?
4. What information sharing processes would you use to disseminate information concerning this incident?
    a. What notification capabilities would you use to share information and communicate protective measures implementation?
    b. How would employee safety concerns be managed (e.g., at what point would the utility company allow employees to enter the site)?
    c. What are your organization's external information sharing responsibilities in response to such incidents?
    d. How would proprietary information concerns be managed?
    e. Are there technological barriers, legal considerations, or institutional sensitivities that might affect information sharing or prohibit use of electronic communication during specific times?
5. What protective security measures would be employed following a domestic attack?
    a. Would you coordinate protective measure implementation with any organization within the Electricity Subsector or specific government entities, such as law enforcement agencies and your CISA PSA?
    b. Would you need to communicate implemented protective measures to organizational liaisons, response entities??
    c. How useful are the information bulletins and advisories the U.S. Department of Homeland Security (DHS) provides (e.g., a JIB) that recommend protective measures?

Final Discussion Questions

1. When is an incident determined to be over?
2. How do you document incident lessons learned?
3. What are your after-action (post-incident) procedures?
4. How do you document and implement improvement plan processes?

ISSN: 2473-4901
v11 n6396

Appendix 2. Scale Items and Confirmatory Factor Analysis.

Scale	Variance explained	Cronbach's Alpha	Items	Factor Loadings
Perceived organizational performance	60.2%	0.862	Our organization exceeded its objectives for dealing with this cyber incident.	0.748
			Reports on our organization's performance in dealing with cyber incidents are favorable.	0.712
			Our organization successfully dealt with this cyber incident.	0.865
			Overall, I am satisfied with the outcome we achieved through the tabletop exercise.	0.749
			Overall, we handled the problems in the tabletop exercise well.	0.802
			I am satisfied with our performance during the tabletop exercise.	0.769
Perceived benefit of the exercise	79.8%	0.865	The tabletop exercise helped my organization acquire new knowledge when dealing with cybersecurity incidents.	0.944
			The table top exercise helped my organization understand its weaknesses when dealing with cybersecurity incidents.	0.834
			The tabletop exercise will benefit my organization.	0.898
Perceived organizational security efficacy	90.4%	0.945	My organization has above-average ability in responding to cybersecurity events.	0.970
			My organization has the resources to respond appropriately to cyber incidents compared to other organizations.	0.947
			The members of my organization have excellent skills for dealing with cyber incidents.	0.935

* Confirmatory Factor Analysis with varimax rotation; N = 43. Variance explained is of the single factor identified in each analysis.

ISSN: 2473-4901
v11 n6396

Appendix 3. Frequencies for Categorical Control Variables.

Variable		N	Valid %
In-person or virtual attendance	In person	43	93.5
	Virtual	3	6.5
Affiliation	CISA	4	8.7
	Electric Company	3	6.5
	Electric Co-op	22	47.8
	National Guard	9	19.6
	NGO	2	4.3
	State/Local Govt	6	13.0
Rank in home organization	Individual Contributor	26	57.8
	Supervisor/Manager	13	28.9
	Director	4	8.9
	VP or SVP	1	2.2
	Top Management Team	1	2.2
Position Tenure	Less than 1 year	5	12.5
	1-3 years	13	32.5
	3-7 years	8	20.0
	7-12 years	4	10.0
	More than 12 years	10	25.0
Age	25-34 years	3	7.7
	35-44 years	17	43.6
	45-54 years	11	28.2
	55-64 years	8	20.5
Gender	Female	9	23.1
	Males	28	71.8
	Non-binary	1	2.6
	Prefer not to respond	1	2.6
Race	Hispanic or Latino	3	7.7
	White	33	84.6
	Prefer not to respond	3	7.7
Veteran status	Not a veteran	36	80.0
	Veteran	6	13.3
	Prefer not to respond	3	6.7