

Strengthening Incident Response: Lessons from Cybersecurity Tabletop Exercises for Rural Critical Infrastructure

Reda Haddouch
Reda.haddouch@umontana.edu

Shawn F. Clouse
shawn.clouse@umontana.edu

Ryan T. Wright
ryan.wright@virginia.edu

Theresa Floyd
theresa.floyd@umontana.edu

Patricia Perry
patricia.perry@umontana.edu

University of Montana
Missoula, MT

Abstract

This case study evaluates the effectiveness of three tabletop exercises (TTXs) that focus on cybersecurity attacks on rural critical infrastructure. By analyzing three distinct TTXs, the researchers identified strengths, weaknesses, and best practices for the three different approaches utilized. This case analysis is categorized based on three inputs (engagement, technology, and facilitation) and two outcomes (collaboration and knowledge gains). The findings highlight the importance of active participation, skilled facilitation, robust technology solutions, and collaboration among state and federal agencies. Further research should expand on participant feedback, involve diverse geographic areas, and explore the human element in cybersecurity to enhance the resilience and security of critical infrastructure systems.

Keywords: Critical infrastructure security, cybersecurity, tabletop exercises, and incident response training.

1. INTRODUCTION

Defending systems and assets that constitute critical infrastructure is vital to the national security, public safety, and economic prosperity of the United States (*National Cybersecurity Strategy*, 2023). The United States continues to face risk to its critical infrastructure from state actors, non-state actors, and criminal networks

as well as insider threats. Rural states are particularly vulnerable due to their limited resources and investment in protecting critical infrastructure. A common, low-cost, and high-impact method for preparing stakeholders for cyberattacks against critical infrastructure is through tabletop exercises (TTXs) (Angafor et al., 2020). Moreover, conducting critical

infrastructure incident response TTXs are a way to practice the coordination, communication, and information sharing protocols between critical infrastructure organizations and partner organizations while responding to hypothetical disruptive cyber and physical incidents (Angafor et al., 2024; Angafor et al., 2020, 2023; Chowdhury et al., 2022; Staves et al., 2022). 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.

This study focuses on the energy and healthcare sectors within rural states in the Rocky Mountain West. It analyzes three TTXs conducted to enhance incident response capabilities in these critical infrastructure sectors. The methodologies used within the TTXs include interdisciplinary planning, scenario development, and the utilization of decision support systems. By examining these exercises, the study aims to identify strengths, weaknesses, and best practices for improving incident response specifically for rural settings.

Literature review

The purpose of this literature review is to gain insights from existing research and best practices in incident response for critical infrastructure in rural areas. The literature review covers incident response for critical infrastructure and the importance of having a disaster recovery plan.

Incident Response for Critical Infrastructure in Rural Areas:

Research conducted by Chowdhury and Gkioulos (2021) highlights the significance of incident response in critical infrastructure sectors. The authors emphasize the need for well-prepared incident prevention teams, particularly in the energy sector, which has been significantly affected by the digitalization of power supply processes. The study recommends workforce management as a domain in the cybersecurity capability maturity model (C2M2) to enhance organizational training and awareness.

In rural areas, incident response for critical infrastructure poses unique challenges due to the distinct characteristics of these regions. The large geographic location, low population density, limited internet connectivity, and limited resources and capabilities necessitate a custom approach and strategy for incident response. While the geographical dispersion of critical infrastructure assets in rural areas poses logistical challenges for incident response teams, rural regions often have limited resources,

including fewer cybersecurity experts, limited network infrastructure, and slower communication channels. Kechagias et al. (2022) discuss the digital transformation of the maritime industry and the associated cybersecurity challenges. Factors such as low visibility, interconnected businesses, and reliance on legacy IT and OT systems that contribute to the vulnerability of critical infrastructure in maritime industry, can also apply to rural sectors. These factors hinder the ability to detect, respond, and recover from cyber incidents promptly.

Cyber exercises and education training need to be customized to address the specific needs and limitations of rural areas and ensure effective incident management. Kick (2014., pp. 8–11) defines three types of cyber exercises: Tabletop exercises (Scripted events), Hybrid exercises (Scripted events with real probes/scans), and Full-life exercises with real scenarios. Tailored approaches and strategies are crucial in addressing these challenges. This includes establishing strong partnerships between critical infrastructure operators, local government agencies, and law enforcement, to enhance information sharing and coordination. It is worth noting that partnership building requires a large level of effort (Carpenter, 2014, p. 6). Furthermore, building local capacity through training and education programs can empower rural communities to respond effectively to cyber threats. Incorporating advanced technologies, such as remote monitoring systems and automated incident response tools, can bolster incident response capabilities in rural areas.

Disaster Recovery Planning:

Disaster recovery planning plays a vital role in ensuring the resilience of critical infrastructure systems. It involves developing comprehensive and adaptable plans to restore normal operations following a disruptive event. The significance of such planning is underscored by the potential for cyber incidents to disrupt the electric grid and other critical infrastructure, causing significant economic and societal consequences. According to Anneli (2006), rural utilities exemplify entities that could be specifically targeted to disrupt critical infrastructure. The author emphasizes that government agencies must be prepared for large-scale disasters and collaborate with local communities (Anneli, 2006, p. 224). Effective disaster recovery planning requires a multi-faceted approach. Comprehensive and adaptable plans are essential to effectively respond to and recover from various disruptive events. According to Wrobel and Wrobel (2009), disaster recovery planning for the electric utility grid seems self-evident (p. 3). The authors

believe that any recovery plan begins with communications. The authors also add that “the ability to garner an immediate situational analysis and report to a responsible decision-making executive is paramount to the process” (p. 11). They continue by explaining that plans tend to change and that any change or deviation requires communication as well.

In addition to communication, effective disaster recovery involves identifying critical assets and their dependencies. The dependencies and interdependencies among critical infrastructures and their cascading effects have been investigated by many authors including Kotzanikolaou et al. (2013) and Palleti et al. (2021). Kotzanikolaou et al. (2013, p. 1) explain that “Protecting Critical Infrastructures (CI) poses challenges not only due to the significant social impact caused by disruption of their services, but also due to the high number of dependencies between them.” Setola et al. (2009, p. 171) highlight that the interdependencies between infrastructure components may exist but are often not easily visible or fully understood by the operators responsible for managing and maintaining the infrastructure.

Moreover, beyond the complexities of identifying critical assets and their dependencies and interdependencies, another crucial aspect of effective disaster recovery is the establishment of backup systems and the implementation of robust data backup and restoration procedures. Backup systems provide a safety net by creating duplicates of critical data and infrastructure components, ensuring their availability in the event of a disruption or loss. By establishing backup systems and implementing reliable data backup and restoration procedures, electrical infrastructure operators can significantly enhance the reliability and resiliency of their systems.

Lastly, regular testing and simulation exercises help validate the effectiveness of the plans and identify areas for improvement. Franchina et al. (2021) explain that a combination of passive, active, and hybrid training techniques can be effective in delivering tailored and engaging training, fostering a security culture, and addressing specific company needs while minimizing disruptions and costs. The study emphasizes the importance of establishing a “human firewall” through Security Education, Training, and Awareness (SETA) programs. Hybrid training techniques, such as tabletop exercises and cyber threat hunting and intelligence, are proposed as effective methods to achieve security awareness. Additionally, close collaboration between government agencies, industry stakeholders, and relevant community organizations is essential to align recovery efforts

and streamline the restoration process (Anelli, 2006; Franchina et al., 2021).

Tabletop Exercises (TTX)

The National Institute of Standards and Technology (NIST 800-84) has long emphasized the necessity for organizations to implement comprehensive incident response plans that encompass the “development and implementation of a test, training, and exercise (TT&E) program” (Grance et al., 2006). According to NIST, tests involve using tools to capture quantifiable metrics specific to the system, such as backup and recovery tests. Training focuses on clearly articulating roles and responsibilities to organizational personnel. Exercises simulate emergency situations to validate one or more aspects of the disaster recovery plan. The most common exercise is tabletop exercise (TTX) which are,

“... discussion-based exercises where personnel meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency situation. A facilitator presents a scenario and asks the exercise participants questions related to the scenario, which initiates a discussion among the participants of roles, responsibilities, coordination, and decision-making. A tabletop exercise is discussion-based only and does not involve deploying equipment or other resources.” (NIST 800-84).

2. METHODOLOGY

The goal of this research project was to explore different methods for conducting critical infrastructure incident response TTXs. This multiple-case study looks at three different methods for conducting incident response tabletop exercises for critical infrastructure. All TTXs were conducted in rural states in the Rocky Mountain West. Two of the cases were in the power or electrical industry and one was for healthcare in a rural state.

All TTX sessions started with an interdisciplinary planning team that organized the event and developed the exercise. The participants included staff from the university, staff from CISA, staff from the states conducting the TTX training, and members from the critical infrastructure organizations. The planning team met several months prior to the event. They developed goals for the TTX, developed the participant list, designed the scenario for the exercise, and a plan to identify gaps during the after-action review. Several of the cases used the DECIDE Platform from Norwich University Applied Research Institutes (NUARI, n.d.) as a decision support system to be used during the exercise. It 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. All exercises had some participants in a face-to-face meeting room as well as others participating virtually via an internet videoconferencing system.

3. DATA COLLECTION AND PROCEDURE

The TTX sessions gathered observation data, comments from the participants, and surveys from the participants. This case study will compare the processes used in the three exercises and the observations made by the researchers. The three exercises will be analyzed on six different aspects of the TTX, which will be used to develop a strengths and weaknesses summary for each case. Taken together, these summaries will form the basis of the recommendations and suggestions for conducting a critical infrastructure incident response exercise in a rural area.

Electrical Grid TTX 1

The first electrical grid TTX was for the entire rural state in the Rocky Mountain West. The group that planned the exercise were from a state university, the governor's office, the state Cybersecurity and Infrastructure Security Agency (CISA) coordinators, National Guard, and some representatives from a public power company and rural electrical cooperatives. The participants in the exercise were the public power company, 20 energy cooperatives, the state fusion center, the Department of Homeland Security, National Guard, and state IT.

The event was held for six hours in two adjoining rooms at the university. There were 29 participants from the power industry and 28 observers from state and federal agencies as well as the National Guard. Most of the participants (51) attended in-person and (6) attended virtually. All participants had laptops that were connected to the NUARI DECIDE Platform. NUARI provided staff to troubleshoot problems and to advance the injections for the exercise. The exercise scenario is described in the Appendix. 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 participants were given 20 minutes for discussion. Then everyone was brought back together for a large discussion for 15 minutes following each step of the TTX. During the 20-minute small group discussion, some players entered comments into the DECIDE platform. 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.

Electrical Grid TTX 2

This TTX was for an electrical region of a different rural Rocky Mountain West state. The group that planned the exercise were from a state university, a regional power company, and power cooperatives from that region. Participants were from the governor's office, a municipal utility, and other regional utilities. The purpose was for power companies and state agencies to collaborate in addressing a cybersecurity attack and to focus on improving and hardening the policies, procedures and resource prioritization across the region in response to the attack. This TTX also had university students, staff, and faculty participate to improve research and education in smart grid technologies and incident response. The event lasted five hours and was conducted in one room with in-person and virtual participants. The room was set up with an inner half circle with leaders (organizational & tech) from the participating power company and cooperatives. The registration list had eight facilitators, 17 players, 21 observers from the power industry, and 18 observers from state agencies, universities, and consulting firms. The final attendees included eight players, nine power industry observers, and 13 observers representing other agencies. Twenty-one attendees participated in person and nine participated virtually via Zoom. The players were

the main participants in the exercise discussion, and they sat in a half circle in the middle of the room. There was a larger outer half circle where power company observers and other observers sat. All players and observers had laptops that were connected to the NUARI DECIDE Platform. NUARI provided staff to trouble shoot problems and to advance the injections for the exercise. The exercise scenario is described in the Appendix. The players in the inner half circle used DECIDE to see the scenario injections and discuss them in the platform. The observers were able to view the content that was posted on DECIDE. After the online discussion, a facilitator led a discussion with all players and observers.

Healthcare TTX 3

This TTX was held for healthcare professionals in a rural state in the Rocky Mountain West. The TTX delivered represented a realistic ransomware security incident for the healthcare industry. It incorporated situations where the healthcare providers would need to reach out to state and federal services to coordinate with and receive assistance. The group that planned the TTX were from a state university, state CISA representatives, the governor's office, and some of the healthcare providers. This exercise did not use the DECIDE Platform and all discussion happened in-person or via Zoom. The exercise lasted four hours and was held in a large room for 59 in-person participants and 76 online participants on Zoom. There were 100 participants representing regional hospitals, rural hospitals, and healthcare clinics throughout the state. There were 26 observers representing the medical associations, healthcare insurance, state and county government, the FBI, the National Guard, and CISA. The face-to-face participants and observers sat at round tables distributed throughout the large room; each table held eight to ten people. The session was facilitated by a national CISA facilitator. The facilitator put the scenario injection on a PowerPoint slide on a screen in the room and talked through what happened to cause security issues. All participants were given time to think about the scenario and discuss at their table before the facilitator led the discussion based on questions for each of the scenario modules. The facilitator asked for comments from both the in-person and virtual audience. The TTX scenario is described in the Appendix. Although mics were used so virtual participants could hear the questions and comments, the in-person participants contributed most of the discussion. State & federal experts on the virtual call responded with their expertise to questions raised by the audience.

3. ANALYSIS

The researchers developed an analytical method to examine the multiple data sources and developed summaries of the strengths and weaknesses for each TTX. The analysis used five aspects of the TTX (see Table 1): three inputs and two outcomes. The inputs categories were selected based on qualitative categorization. The outcomes were garnered from past TTX research which argue that collaboration and knowledge gain are critical outcomes (Frégeau et al., 2020). The aspects are as follows:

1. **Engagement:** Engagement and participation levels indicate how involved and invested the participants were during the exercises. High levels of engagement guarantees that participants are both learning and contributing, which is needed for effective TTXs.
2. **Facilitation:** Facilitators are critical in guiding discussions, maintaining overall group focus, and ensuring that all participants are contributing effectively. Effective facilitators directly impact the overall quality of the TTX and directly impact outcomes for participants.
3. **Technology:** Technology platforms, such as the NUARI DECIDE Platform, are common in TTXs. Evaluating the use of these platforms can help our understanding of their strengths and weakness in different TTX contexts.
4. **Knowledge Gains:** According to Frégeau et al. (2020) TTXs increase participants' knowledge while also preparing participants to respond to real-world incidents.
5. **Collaboration:** Key to success TTX is the practice gained in dynamic incidents that require quick and effective collaborative. Effective collaboration includes exploring how to effectively communicate with multiple stakeholders while also understanding why participants need effective strategies for communications

Table 1. Evaluation of TTXs			
Aspect	TTX 1: Electrical Grid (State)	TTX 2: Electrical Grid (Regional)	TTX 3: Healthcare (Multi - Regional)
INPUTS: Engagement	<ul style="list-style-type: none"> • Small group - High engagement • Virtual participants - lower engagement • Issues with the DECIDE Platform. 	<ul style="list-style-type: none"> • Participants - Knowledgeable and engaged • Observers - limited participation • Virtual participants - less active. 	<ul style="list-style-type: none"> • Large group size limited individual participation.
INPUTS: Facilitation	<ul style="list-style-type: none"> • Small group - Effective facilitation • Virtual participants - Challenges in managing engagement. 	<ul style="list-style-type: none"> • Facilitators - led focused discussions effectively • Facilitators - struggled to integrate virtual participants. 	<ul style="list-style-type: none"> • Facilitator - Engaged state and federal experts effectively, virtual participants less active. • Facilitator - Successfully involved experts and guided discussions.
INPUTS: Technology	<ul style="list-style-type: none"> • DECIDE Platform - Technical issues • DECIDE Platform - Underutilized by some participants. 	<ul style="list-style-type: none"> • DECIDE Platform - Better utilization compared to TTX 1 • DECIDE Platform - some technical issues. 	<ul style="list-style-type: none"> • DECIDE Platform - Not Used; relied on traditional facilitation methods and physical presence.
OUTCOME: Knowledge Gains	<ul style="list-style-type: none"> • Participants - Gained knowledge on handling cyber incidents, • Participants - Smaller cooperatives learning from larger companies. 	<ul style="list-style-type: none"> • Increased knowledge and preparedness among participants with prior experience in cybersecurity exercises. 	<ul style="list-style-type: none"> • Enhanced understanding of ransomware attacks • Enhanced response strategies among healthcare providers with valuable input from state and federal experts.
OUTCOME: Collaboration	<ul style="list-style-type: none"> • Strengthened relationships • Strengthened collaboration 	<ul style="list-style-type: none"> • Effective collaboration among regional stakeholders. • Limited observer participation. 	<ul style="list-style-type: none"> • Improved communication • Improved collaboration within the healthcare sector and with state and federal agencies.

State Electrical Grid TTX 1 Summary

The TTX had rich data that was entered into the DECIDE platform as well as captured by the scribes. The nine small interdisciplinary groups allowed for rich discussion in the small groups and maximum participation. The large group discussion at the end of each module in the TTX brought all the concepts together and the facilitators made sure that everyone was on the same page with take aways from the module. There was a wide range of cybersecurity

understanding and preparation across all the participants. The coops learned from the power company and vice versa because the coops had different perspectives on how they run their business. The state and federal government participants met and developed relationships with the participants in the power industry, which will facilitate future interaction and collaboration. This TTX had a facilitator to lead the discussion with the virtual participants. It was critical to keep the virtual participants engaged. Even with

a facilitator there were some virtual participants that had their computers in the Zoom session, but they didn't interact at all during the discussions. The virtual participants rarely interacted during the large group module summary discussions. Interestingly, most of the participants chose not to use the DECIDE platform and many complained that it was an extra step that kept them from discussing with their group.

Regional Electrical Grid TTX 2 Summary

Similar to TTX 1, the exercise had rich data that was entered into the DECIDE platform by a limited number of players and summarized by the scribes. The group of players were very knowledgeable and had rich discussions that the observers could monitor. This TTX utilized the DECIDE platform more than TTX1. The facilitators did a great job of leading the broad group discussion related to the questions for each of the scenario modules. The players were very knowledgeable of cybersecurity and how to deal with a security incident for the power industry and most had participated in other tabletop exercises. The observers learned from the discussion by the players, but they didn't actively participate to the level of the players. The state and federal government participants met and developed relationships with the players and observers, which will facilitate future interaction and collaboration. This TTX did not have a facilitator to actively seek discussion from the virtual participants, who had a passive role in the exercise. The virtual participants rarely interacted during the exercise. It is difficult for a face-to-face facilitator to actively lead a discussion between in-person and virtual participants.

Healthcare TTX 3 Summary

This TTX had minimal small group interaction and discussion was facilitated by one facilitator in a large room with both in-person and virtual participants. The participants in the room had to wait for someone to bring a microphone to them to add to the discussion. This TTX had over 100 participants both in the room and online. It is hard to have broad participation with that large of group. The facilitator did an excellent job of calling on federal and state agency experts that were attending virtually, to respond to questions in the exercise as well as questions posed by participants that worked in healthcare. The facilitator also asked pointed questions to solicit responses from both healthcare and state and federal participants. These discussions helped make sure that everyone was on the same page with the steps to take in each of the modules. Some of the healthcare providers had broad

knowledge on how to deal with a ransomware attack and most of the smaller providers had minimal knowledge. The state and federal agency participants provided great insight on what the healthcare industry should do during each of the modules. The TTX provided the opportunity for all the healthcare participants to learn from each other. This exercise also provided the opportunity for healthcare providers to develop relationships within that systems as well as with the state and federal agencies that they would need to work with to recover from a ransomware attack that stopped access to critical systems and to patient records. The virtual government participants were more active in this TTX than the virtual healthcare participants.

Best Practice for Critical Infrastructure Exercises

The analysis of the three distinct TTXs has provided a unique dataset from which to develop both best practices and recommendations. First, it is important to state that all TTXs in this case study had strong positive outcomes and improved both collaboration and knowledge. That said, there were some opportunities to improve aspects of these TTXs.

1, Types of Participation: Critical to successful and impactful TTX is participation. To maximize participation, it is essential to provide many opportunities for individuals to communicate and interact both with the facilitator and with each other. This is particularly important for virtual attendees. Digital platforms can significantly enhance participation by allowing and facilitating easy communication. While technology such as Zoom is commonplace for hybrid (in-person and online) interactions, these technologies require considerable care. The authors recommend appointing a separate in-person and online facilitator at a minimum to ensure both groups' active participation.

2. Facilitation: Effective facilitation is also critical to a successful TTXs. The authors suggest breaking large groups into smaller ones to greatly enhance participation. Large discussion groups are somewhat ineffective in TTXs. Moreover, for large TTX with many smaller groups it is important to summarize what was discussed in the small groups. This step helps in consolidating the conversations and ensures wider knowledge gain. Finally, facilitators need to be inclusive by soliciting comments from all participants, especially those who have not effectively participated. This is especially important in hybrid environments.

3. Use of Technology: Technology can be an important enabler for communications while also capturing data that can be used for analysis later.

These platforms need to be tested thoroughly to ensure they are reliable, as without a proper understanding of the capabilities of the technology platform will be a distraction. Much like high quality incident response strategies, it is important to have an analog backup that can be utilized immediately if the technology platform fails. In sum, it is recommended to test technology solutions along with analog contingency plans.

4. Stakeholders: Both state and federal participation are key to the success of TTXs. Government agencies participation in critical infrastructure TTXs ensures that organizations that are impacted by an incident both know who to contact and how to communicate with government agencies. Further, engaging with government agencies during the TTX provides insights and resources that can help organizations improve their incident response plans. Additionally, this organization will foster stronger relationships and communication channels with government agencies.

Similar to building relationships with governmental agencies, it is important to build relationships with other regional stakeholders. Observer participation from regional stakeholders was limited when involved in the TTX. Efforts need to be made to involve them and integrate their insights into the TTX. When participants do not have active roles in the TTX, their engagement, knowledge gains, and collaboration are limited. In sum, the sideline observer strategy was found to be ineffective in this case study.

Limitations and Opportunities for future research

First it is important to note that the data from this case study is based solely on observations made by the researchers who participated in the three TTXs. The exercises were all focused on rural environments in the Rocky Mountain West, which have limited resources to combat cybersecurity attacks. Consequently, readers should proceed with caution when generalizing these takeaways to other ecosystems. Future research should study critical infrastructure in non-rural contexts as well as expand beyond electrical grid and healthcare. The DECIDE platform that was used in two of the TTX was a limitation and future research should look at how decision support systems can be used effectively in critical infrastructure incident response exercises.

Future research should expand beyond the observations of the three TTXs to include a broader range of methodologies, participant feedback, and contexts (e.g., other rural sectors such as agriculture or water management). Key

areas for further investigation include surveying participants to assess their security knowledge before and after exercises, providing valuable insights into the effectiveness of the training. Conducting social network analysis can identify the most effective communication and response networks during critical infrastructure security events, enhancing coordination and response efforts. The human element is critical to cybersecurity and future research should explore how human factors impact the outcomes of TTXs. Involving researchers in the planning stages of tabletop exercises is crucial to ensure buy-in from all parties and facilitate data collection, especially as securing a sample of leaders and technical employees in critical infrastructure is challenging but essential for comprehensive research. This action research approach is a viable option that produces high quality outcomes in the organization (Altrichter et al., 2002).

Further, performing qualitative analysis of discussion transcripts from the exercises will help develop best practices by understanding the nuances of participant interactions and decision-making processes. Measuring participant satisfaction with the tabletop exercises is also vital for identifying strengths and areas for improvement. Finally, it was clear from the exercises that more research is needed on the importance of the "Human Firewall," emphasizing the human element in preventing security breaches. Understanding the role of human behavior and decision-making is as important as the technical aspects of critical infrastructure protection (Koza, 2022).

4. REFERENCES

- Altrichter, H., Kemmis, S., McTaggart, R., & Zuber-Skerritt, O. (2002). The concept of action research. *The Learning Organization*, 9(3), 125–131. <https://doi.org/10.1108/09696470210428840>
- 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>
- Angafor, G. N., Yevseyeva, I., & Maglaras, L. (2023). Scenario-based incident response training: Lessons learnt from conducting an experiential learning virtual incident response tabletop exercise. *Information & Computer Security*, 31(4), 404–426. <https://doi.org/10.1108/ICS-05-2022-0085>
- Angafor, G., Yevseyeva, I., & Maglaras, L. (2024). MalAware: A tabletop exercise for malware security awareness education and incident response training. *Internet of Things and*

- Cyber-Physical Systems*, 4, 280–292.
<https://doi.org/10.1016/j.iotcps.2024.02.003>
- Anelli, J. F. (2006). The national incident management system: A multi-agency approach to emergency response in the United States of America. *Revue Scientifique et Technique de l'OIE*, 25(1), 223–231.
<https://doi.org/10.20506/rst.25.1.1656>
- Carpenter, A. M. (2014). Critical infrastructure resilience: A baseline study for Georgia. *ICSI 2014: Creating Infrastructure for a Sustainable World ASCE 2014*, 186–197.
<https://doi.org/10.1061/9780784478745.017>
- Chowdhury, N., & Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, 40, 100361.
<https://doi.org/10.1016/j.cosrev.2021.100361>
- Chowdhury, N., Nystad, E., Reegård, K., & Gkioulos, V. (2022). Cybersecurity Training in Norwegian Critical Infrastructure Companies. *International Journal of Safety and Security Engineering*, 12(3), 299–310.
<https://doi.org/10.18280/ijss.120304>
- Franchina, L., Inzerilli, G., Scatto, E., Calabrese, A., Lucariello, A., Brutti, G., & Roscioli, P. (2021). Passive and active training approaches for critical infrastructure protection. *International Journal of Disaster Risk Reduction*, 63, 102461.
<https://doi.org/10.1016/j.ijdrr.2021.102461>
- Frégeau, A., Cournoyer, A., Maheu-Cadotte, M.-A., Iseppon, M., Soucy, N., Bourque, J. S.-C., Cossette, S., Castonguay, V., & Fleet, R. (2020). Use of tabletop exercises for healthcare education: A scoping review protocol. *BMJ Open*, 10(1), e032662.
<https://doi.org/10.1136/bmjopen-2019-032662>
- 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>
- Kechagias, E. P., Chatzistelios, G., Papadopoulos, G. A., & Apostolou, P. (2022). Digital transformation of the maritime industry: A cybersecurity systemic approach. *International Journal of Critical Infrastructure Protection*, 37, 100526.
<https://doi.org/10.1016/j.ijcip.2022.100526>
- Kick, J. (n.d.). *Cyber Exercise Playbook*.
- Kotzanikolaou, P., Theoharidou, M., & Gritzalis, D. (2013a). Assessing n-order dependencies between critical infrastructures. *International Journal of Critical Infrastructures*, 9(1/2), 93.
<https://doi.org/10.1504/IJCIS.2013.051606>
- Kotzanikolaou, P., Theoharidou, M., & Gritzalis, D. (2013b). Interdependencies between Critical Infrastructures: Analyzing the Risk of Cascading Effects. In S. Bologna, B. Hämmerli, D. Gritzalis, & S. Wolthusen (Eds.), *Critical Information Infrastructure Security* (Vol. 6983, pp. 104–115). Springer Berlin Heidelberg.
https://doi.org/10.1007/978-3-642-41476-3_9
- Koza, E. (2022). *Information security awareness and training as a holistic key factor – How can a human firewall take on a complementary role in information security?* 13th International Conference on Applied Human Factors and Ergonomics (AHFE 2022).
<https://doi.org/10.54941/ahfe1002201>
- National Cybersecurity Strategy. (2023). The White House.
<https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>
- NUARI: Addressing National Cyber Security Issues. (n.d.). Retrieved September 7, 2024, from <https://nuari.org>
- Palleti, V. R., Adepur, S., Mishra, V. K., & Mathur, A. (2021). Cascading effects of cyber-attacks on interconnected critical infrastructure. *Cybersecurity*, 4(1), 8.
<https://doi.org/10.1186/s42400-021-00071-z>
- Setola, R., De Porcellinis, S., & Sforza, M. (2009). Critical infrastructure dependency assessment using the input-output inoperability model. *International Journal of Critical Infrastructure Protection*, 2(4), 170–178.
<https://doi.org/10.1016/j.ijcip.2009.09.002>
- Staves, A., Anderson, T., Balderstone, H., Green, B., Gouglidis, A., & Hutchison, D. (2022). A Cyber Incident Response and Recovery Framework to Support Operators of Industrial Control Systems. *International Journal of Critical Infrastructure Protection*, 37, 100505.
<https://doi.org/10.1016/j.ijcip.2021.100505>
- Wrobel, L. A., & Wrobel, S. M. (2009). *Disaster recovery planning for communications and critical infrastructure*. Artech House.

APPENDIX

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 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 federal government (specific organizations) to enhance state, local government, and industry

Training Objectives per Organization:

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 process to request for 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 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 approval process for cyber incident response (ie: 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 inject, 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 providers 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 members 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 provider 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. Would any of the events described in this module be identified as cybersecurity incidents? If so, how would 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?

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 a level transformer 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 these 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 to 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 this incident?
 - 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?

Electrical Grid TTX 2 Modules and Questions

AGENDA for Electrical Grid TTX2

- 8:00:00 AM MDT: Join Zoom!
- Login to DECIDE® Exercise Platform
- Welcome and Scene Setter
- Time to answer Pre-Exercise survey questions in DECIDE
- 8:15 AM: Begin Exercise with Turn 1: Injects, Discussion, Survey
- 8:55 AM: Break
- 9:00 AM: Restart Exercise. Turn 2: Injects, Discussion, Survey
- 9:55 AM: Break
- 10:00 AM: Restart Exercise. Turn 3: Injects, Discussion, Survey
- 10:55 AM: Break
- 11 :00 AM: Restart Exercise. Turn 4: Injects, Discussion, Survey
- 11 :55 AM: Break
- 12:00 PM: WORKING LUNCH: Hotwash, Closing Comments
- 1 :00 PM: End Exercise

Purpose of this Exercise:

This exercise is designed to strengthen the infrastructure and response of State energy and utility participants in light of a cyber-attack. We will use the DECIDE platform to simulate a persistent malware attack against utilities. Participants (the Governor's Office of Information Technology, State utilities, and other regional utilities) will collaborate in addressing the attack with a focus on improving and hardening the policies, procedures and resource prioritization across the region in response to the attack. In addition, university students, staff, and faculty will participate to drive improved research and education in smart grid technologies and incident response.

What is DECIDE®?

DECIDE® is a platform initially conceived and started independently by NUARI and developed with funding from the Department of Homeland Security. The DECIDE® platform has been a trusted cybersecurity live exercise solution for more than ten years. DECIDE® equips organizations, critical infrastructure sectors, the military, and the government with the situational awareness, strategic communications capabilities, and digital response playbooks needed to prevail against serious cyber threats.

Objectives

The exercise objectives in Table 2 describe the expected outcomes for the exercise. The objectives are linked to capabilities, which are distinct critical elements necessary to achieve the specific focus area(s). The objectives and aligned capabilities are guided by senior leaders and selected by the Exercise Planning Team.

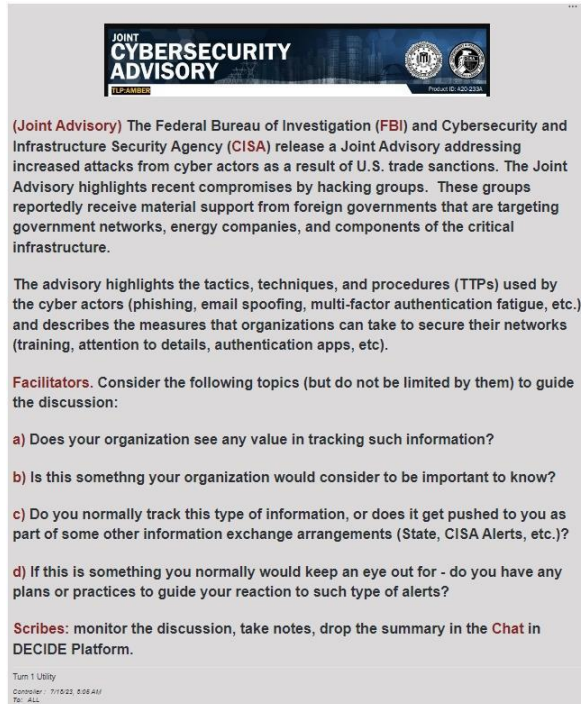
Exercise Objectives	FEMA Core Capability
Establish a collaborative structure across county, city, and state utilities such that both communication coordination and investigation collaboration with outside agencies is open and aligned to build on one another's efforts and will avoid duplication and inefficiency.	Intelligence and Information Sharing Operational Communications
Exercise the state's, cities', and energy/utility sector's ability to improve critical SmartGrid infrastructure incident response and escalation response, and to discover gaps and enhance resilience, especially as it relates to interaction, coordination, and communication across the state.	Infrastructure Cybersecurity Systems

Explore current emergency management policies and practices as they relate to municipal and regional (city, county, state) energy and utility SmartGrid infrastructure. Define/refine priorities – what needs are addressed first in an emergency – based on new policy across these organizations and the region	Situational Assessment
---	------------------------

Facilitators must ensure that the participants are given enough time to read the injects.

Turn 1: Scene Setter

- Joint Advisory alert and Sanctions



JOINT CYBERSECURITY ADVISORY
FBI CISA
Product ID: 4022331

(Joint Advisory) The Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) release a Joint Advisory addressing increased attacks from cyber actors as a result of U.S. trade sanctions. The Joint Advisory highlights recent compromises by hacking groups. These groups reportedly receive material support from foreign governments that are targeting government networks, energy companies, and components of the critical infrastructure.

The advisory highlights the tactics, techniques, and procedures (TTPs) used by the cyber actors (phishing, email spoofing, multi-factor authentication fatigue, etc.) and describes the measures that organizations can take to secure their networks (training, attention to details, authentication apps, etc).

Facilitators. Consider the following topics (but do not be limited by them) to guide the discussion:

- a) Does your organization see any value in tracking such information?
- b) Is this something your organization would consider to be important to know?
- c) Do you normally track this type of information, or does it get pushed to you as part of some other information exchange arrangements (State, CISA Alerts, etc.)?
- d) If this is something you normally would keep an eye out for - do you have any plans or practices to guide your reaction to such type of alerts?

Scribes: monitor the discussion, take notes, drop the summary in the **Chat** in DECIDE Platform.

Turn 1 Utility
Controller: 7/10/23, 0:08:41
To: All



SANCTIONS

(International Sanctions Announcement) The U.S. reinforces economic and trade sanctions on a foreign country, citing currency manipulation, human rights abuses, and a violation of international treaties. Officials from the foreign country vow a “crushing response to U.S. bullying” after the announcement.

Facilitators. Consider the following topics (but do not be limited by them) to guide the discussion:

- a) Does your community (jurisdiction, local government, local OEM, local LE, etc.) see any value in tracking such information?
- b) Is this something your community would consider to be important to know?
- c) Do you normally track this type of information, or does it get pushed to you as part of some other information exchange arrangements (State, CISA Alerts, etc.)?
- d) If this is something you normally would keep an eye out for - do you have any plans or practices to guide your reaction to such type of alerts?
- e) If this is something you normally would keep an eye out for - would you consider pushing this information down to your community lifelines?

Scribes: monitor the discussion, take notes, drop the summary in the **Chat** in DECIDE Platform.

Turn 1 Community

- Indicators of Compromise (IOC)

On July 17, 2023 electric generation plant operators begin to notice that processes are failing and becoming unresponsive. When investigating the cause, maintenance staff narrow the problem down to inoperable process controller systems.

They discover that process controller hardware is powered on but is completely unresponsive and inputs and outputs appear to be dead.

While troubleshooting the initial processes that failed, many other plant processes go offline with their controllers also becoming unresponsive.

Maintenance staff attempt several methods to bring the controllers back online, to include restoring from backups and resetting to factory defaults.

All attempts are unsuccessful, and the controller appear to be “bricked.” Somewhere during this troubleshooting process, the plant can no longer be safely controlled and operators have brought it offline.

Also, during this time, any other generating plants operated by the utility are seeing the same impacts and are also being brought offline.

Discussion topics to consider (**Scribes**, capture the summary of what is being said and drop it in the **Chat** for future review):

- a) What would be some of the warning signs of this unfolding disaster?
- b) Who (organization, department, and/or position) would most likely be the first ones to catch this , and what actions are they expected to take upon such discovery?
- c) PPROEM has a very robust immediate response checklist. What if the situation is caught by one of the utilities - are there similar response procedures in place?
- d) At what point of this scenario would the utilities reach out for help? At what point would the utilities start notifying other power pool utilities, state and federal agencies, PUC, NERC, etc?

Turn 1 Scene Setter

Controller : 7/15/23, 8:40 AM
To: NUARI (Observer), NUARI (Controller), Colorado Focal (Reviewer), Colorado Focal (Player), Colorado Focal (Observer)

Turn 2: Scripted Response

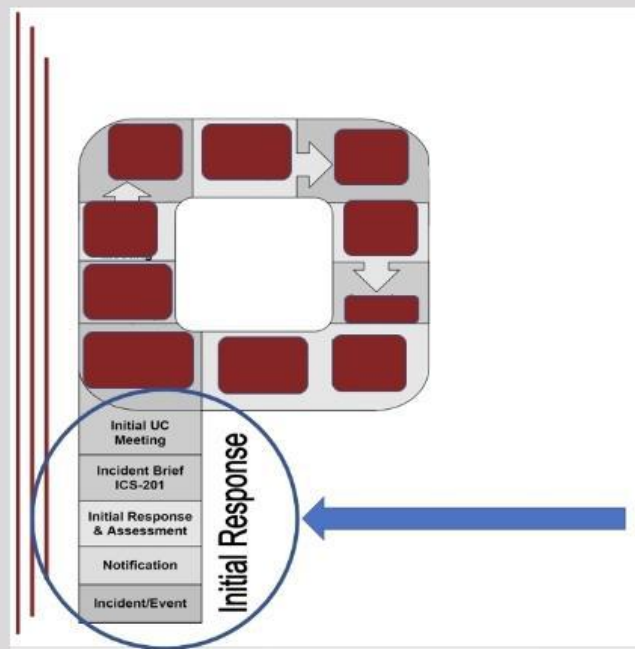
- Incident Response Plan (IRP) evaluation, application, and implementation

RELATED QUESTIONS ...

UTILITY: In this module we would like to discuss your "**scripted**" response actions. The incident happened, or is happening as we speak. How does your organization respond?

Lets talk about following your currently existing IRP and/or response checklist(s). Do you have one? Is it clearly written? What actions, according to your current IRP are you taking at this time?

In terms of Incident Command System - you are now in the stem portion of the Planning P process.



Turn 3: Mature Response

- Executive and political leadership involvement, decision-making exploration and evaluation

The initial local level response is taking place. All necessary notifications have been made, the ECC has been activated and is running.

The current **PPROEM** response plan presents a very well-written checklist of actions to take. It also mentions utilization of various ICS forms, such as 214 and 213RR. Are the utilities trained on the ICS terminology and processes? Will they be able to communicate in the same language as the ECC?

While the individual utilities are busy with the immediate response actions, ECC is making decisions, identifying objectives, handling internal and external notifications, etc.

There is a good possibility that the competitors from the adjoining communities will try to step in and remain operating on your utilities' turf - is this something worthy of discussing?

In the event if the power delivery cannot be immediately restored to all community lifelines, but can be restored to some - who makes the decisions about power distribution?

What topics do you believe are appropriate to discuss at this time?

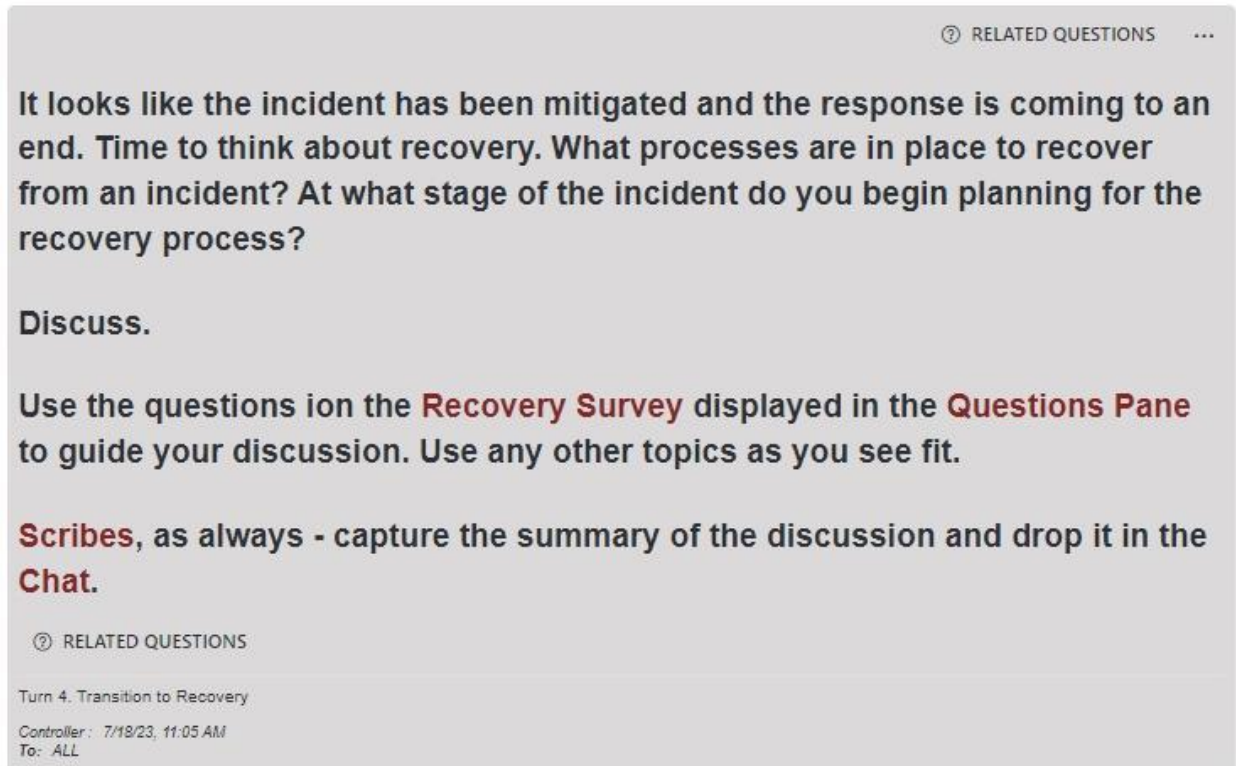
Please follow the Mature Response Survey in the **Questions Pane** to use as guidance for the discussion, or feel free to use your own topics if they are more appropriate.

Scribes, as always, please make sure to capture the summary of the discussion and drop it in the **Chat** for later review.

🔗 RELATED QUESTIONS

Turn 4: Transition to Recovery

- Exploration and evaluation of the current recovery processes



The screenshot shows a discussion prompt within a platform interface. At the top right, there is a link for "RELATED QUESTIONS" with a question mark icon and three dots. The main text of the prompt reads: "It looks like the incident has been mitigated and the response is coming to an end. Time to think about recovery. What processes are in place to recover from an incident? At what stage of the incident do you begin planning for the recovery process?" Below this, it says "Discuss." and provides instructions: "Use the questions on the Recovery Survey displayed in the Questions Pane to guide your discussion. Use any other topics as you see fit." It also instructs: "Scribes, as always - capture the summary of the discussion and drop it in the Chat." At the bottom of the prompt area, there is another "RELATED QUESTIONS" link, the title "Turn 4. Transition to Recovery", and metadata: "Controller: 7/19/23, 11:05 AM" and "To: ALL".

NOTE: When presented in DECIDE® Platform, each inject will be accompanied by suggested discussion topics. Additional discussion topics will be displayed in the form of questions in the Questions Pane. Facilitators may choose to utilize these topics to lead the discussion as they see fit.

Exercise Structure

Control of the exercise is accomplished through an exercise control structure. The control structure is the framework that allows Facilitators to communicate and coordinate with other Facilitators and Evaluators to deliver and track exercise information. The control structure for this exercise is simplified to allow for the all-inclusive discussion.

The composition of the exercise participants will be as follows:

- Facilitator(s)
- Players
- Scribes

Healthcare TTX 3 Modules and Questions

Exercise Purpose:

Examine cyber incident planning, preparedness, identification, and response among rural healthcare organizations.

Objectives:

- 1) Examine the state's healthcare organization's ability to detect, respond to, and recover from a significant cyber incident.
- 2) Discuss the impacts of a cyber incident on state's healthcare organization's ability to maintain and continue patient care and business continuity.
- 3) Explore the state's healthcare organization's processes for information sharing and communications during a cyber incident.
- 4) Increase understanding of available state and federal resources.
- 5) Discuss vulnerabilities to external dependencies and examine how to mitigate them.

Module 1

September 1: The Department of Health and Human Services (HHS) Health Sector Cybersecurity Coordination Center (HC3) sends out an alert warning of a novel ransomware-as-a-service (RaaS) group that is targeting multiple sectors, including the Health and Public Health (HPH) sector, by launching phishing attacks and utilizing Sliver to breach networks.

October 2: The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) distributes a joint cybersecurity advisory that warns of the novel Hydra RaaS group and reinforces the HC3 alert. The advisory includes the common tactics, techniques, and procedures (TTPs) used by the group.

October 13: Multiple healthcare facilities and vendors across state receive an email from a cybersecurity firm about HPH sector cyber threats and hazards. The email includes an attached PDF fact sheet that lists several mitigations users can implement to reduce their risk of a cyberattack. The firm is not known across the state, but the fact sheet is not seen as suspicious.

October 18: Administrative staff at several different healthcare facilities report issues accessing files on their computers. A few files load slowly, especially files that are located on shared drives. Nursing staff also report that certain pages within the electronic medical records (EMR) system are taking an unusually long period of time to load.

Discussion Questions

- 1) Describe what cybersecurity threat information your organization receives and how it is shared.
- 2) What actions would you take based on the alert?
- 3) Describe your organization's cybersecurity training program.
 - a) How often are employees required to complete training?
 - b) What additional training is required for employees who have system administrator-level privileges?
 - c) What type of training methods or approaches have you found most beneficial?
- 4) How do employees report suspected phishing attempts?
- 5) What process would your organization's IT department follow when suspicious emails are reported?
- 6) Describe what actions you would take based on the reports of issues with the EMR system and administrative staff not being able to access files?

Module 2

October 22 – Morning: A large Clinic experiences issues with the doors within their facility. The doors that require badge access to open, primarily between waiting rooms and treatment areas, do not open when a badge with valid certificates is swiped. Staff at the front desk notify security and facilities about the issues with the doors.

October 22 – Noon: Medicine dispensing equipment at multiple healthcare facilities across the state experience issues with their ability to calculate dosage. Nurses are still able to retrieve their required medicine, but they must calculate dosages themselves.

October 23 – Morning: Multiple healthcare vendors report to their clients that they have been the victim of a cyberattack. They provide no further details other than they are investigating the issue and will notify their clients when they learn more.

October 23 – Afternoon: Stock in the medicine dispensing equipment at multiple healthcare facilities is running low on stock. Nurses are unable to submit requests for more medication electronically and must physically go to the pharmacy to place orders and retrieve medicine. Patients are not receiving medication on time due to issues with the badged access doors throughout select facilities.

October 24: A university’s nursing school administration office notifies your healthcare facility that they have detected a network intrusion through several of their nursing students’ accounts. They detected this intrusion after several students complained they were unable to maintain a virtual private network (VPN) connection with your healthcare organization.

Discussion Questions

- 1) Based on the scenario, what are your priorities at this point?
- 2) Describe how IT coordinates with physical security as it relates to the issue with the doors.
 - a) Would there be any additional concerns with physical security of the healthcare facility due to the door issue?
- 3) When would your organization activate their business continuity plan?
 - a) Describe how the state’s Department of Public Health and Human Services would interact with your organization during these events.
- 4) What level of access do your third-party vendors have to your organization’s network?
- 5) Describe your downtime procedures.
 - a) How often are your downtime procedures updated and exercised?
 - b) How long can your organization sustain manual/alternate processes when critical systems are not available?
- c) What is your process for updating systems once they are restored?
- 6) When was the last time your medical equipment software was updated?
 - a) Are vendors required to notify your organization prior to installing patches/updates?
- 7) Describe the actions your organization would take upon learning about compromised student accounts.
- 8) What processes do you have to ensure that your external dependencies are integrated into your security and continuity planning programs?
- 9) What are you communicating with the staff, patients and their families, and the public?
 - a) What are you communicating with senior leaders?
 - b) How are senior leaders involved in the development and dissemination of internal and external messaging?

Module 3

October 25 – Morning: Files on computers at multiple healthcare facilities and at the state Department of Public Health and Human Services are missing or had their file names changed. The files that remain include the extension .hydra. A PDF file titled “CriticalBreachDetected.pdf” includes a ransom note stating that systems are encrypted, and data has been exfiltrated.

October 25 – Noon: Multiple healthcare facilities across the state have the same PDF file on their computers and are unable to access key systems to pull patient records or schedule appointments. Staff begin canceling patient appointments, including for those patients who have already arrived at the hospital, causing frustration and complaints.

October 26: The news media reports on the alleged cyberattack at multiple healthcare facilities across the state.

October 27: A professor at a university discovers that the Hydra RaaS group has posted on their TOR page a list of the vendors and healthcare organizations in the state from which they have exfiltrated data, claiming it was their largest “cybersecurity team” effort yet. They post samples of the data that they have exfiltrated as evidence.

Discussion Questions

- 1) Explain your organization’s decision-making process regarding ransomware payment.

- a) Are ransomware policies/procedures included in any of your plans?
- b) Explain how external partners (e.g., cyber insurance, third-party vendors) are included in your procedures.
- 2) What are your data backup and recovery capabilities?
 - a) How often are backups stored and where?
 - b) How quickly can systems be restored from backups?
 - c) How often are backups tested and verified?
 - d) How can you verify the integrity of backed-up data?
- 3) Describe your organization's procedures for enacting your Crisis Communications Plan to respond to the media reports.
 - a) What pre-scripted messages have been developed for cyber incidents?
 - b) What training do your communications personnel receive on cyber terminology?
 - c) How would public messaging be coordinated and disseminated during a cyber incident?
 - 4) What regulatory reporting requirements would your organization need to follow due to the data breach?
 - 5) How would you preserve and reinforce the public's confidence and trust in the state's healthcare system during and after a significant cyber incident?
 - 6) What additional concerns have the incidents described in this scenario generated that have not been addressed in today's discussion?
 - 7) Based on this discussion, what changes would you implement within your organization to increase cyber preparedness?