CYBERSECURITY PEDAGOGY & PRACTICE JOURNAL

**Volume 4, No. 2**
October 2025
ISSN: 2832-1006

In this issue:



iscap
Information Systems & Computing Academic Professionals

The **Cybersecurity Pedagogy and Practice Journal** (**CPPJ**) is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is two times per year. The first year of publication was 2022.

CPPJ is published online (https://cppj.info). Our sister publication, the proceedings of the ISCAP Conference (https://proc.iscap.info) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the ISCAP conference. At that point, papers are divided into award papers (top 15%), and other accepted proceedings papers. The other accepted proceedings papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the CPPJ journal.

While the primary path to journal publication is through the ISCAP conference, CPPJ does accept direct submissions at https://iscap.us/papers. Direct submissions are subjected to a double-blind peer review process, where reviewers do not know the names and affiliations of paper authors, and paper authors do not know the names and affiliations of reviewers. All submissions (articles, teaching tips, and teaching cases & notes) to the journal will be refereed by a rigorous evaluation process involving at least three blind reviews by qualified academic, industrial, or governmental computing professionals. Submissions will be judged not only on the suitability of the content but also on the readability and clarity of the prose.

Currently, the acceptance rate for the journal is under 35%.

Questions should be addressed to the editor at editorcppj@iscap.us or the publisher at publisher@iscap.us. Special thanks to members of ISCAP who perform the editorial and review processes for CPPJ.

# CYBERSECURITY PEDAGOGY AND PRACTICE JOURNAL

## Editors



## 2025 Review Board

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

Reda M. Haddouch
reda.haddouch@umontana.edu

Shawn F. Clouse
shawn.clouse@umontana.edu

Ryan T. Wright
ryan.wright@virginia.edu
University of Virginia
Charlotteville, VA 22903

Theresa M. Floyd
theresa.floyd@umontana.edu

Victor C. Valgenti
victor.valgenti@umontana.edu

Patricia Akello
patricia.akello@umontana.edu

Thomas P. Gallagher
thomas.gallagher@umontana.edu

University of Montana
Missoula, MT 59812

**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 approaches. 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:** Rural critical infrastructure security, cybersecurity, tabletop exercises, and incident response training.

**Recommended Citation:** Haddouch, R., Clouse, S.F., Wright, R., Floyd, T., Valgenti, V., Perry, P., Gallagher, T., (2025). Strengthening Incident Response: Lessons from Cybersecurity Tabletop Exercises for Rural Critical Infrastructure. *Cybersecurity Pedagogy and Practice Journal.* v4, n2, pp 4-35. DOI# https://doi.org/10.62273/10.62273/SACF5628

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

*Reda Haddouch, Shawn F. Clouse, Ryan Wright, Theresa Floyd, Victor Valgenti, Patricia Perry and Tom Gallager*

## 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 risks 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 research project explored different methods for conducting critical infrastructure incident response TTXs, focusing 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 in rural settings.

### Literature review

The literature review covers incident response for critical infrastructure, the importance of disaster recovery plans, and cybersecurity human factors.

### Incident Response for Critical Infrastructure in Rural Area

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. A major risk to critical infrastructure is that industrial control systems are now connected to networks in the same way as enterprise information technology (Malatji et al., 2021). Berkeley et al. (2010) studied the power industry and found that the electrical grid is critical for economics, national security, public safety, and quality of life. Several studies found that it is important for the electrical grid industry to evaluate its resilience against cyber-attacks because of the interconnectivity of information technology and industrial control system systems (Berkeley et al., 2010; Ota et al., 2022). Christiansen (2022) stressed the importance of critical infrastructure to build an incident response team with executive management support and conduct tabletop exercises at least quarterly. These exercises help educate team members on the complexity of a cyber-attack.

In rural areas, incident response for critical infrastructure poses unique challenges due to the distinct characteristics of these regions. The large geographic area, 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 also

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 operational technology (OT) systems that contribute to the vulnerability of critical infrastructure in the 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 (Annelli, 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. They 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.

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) highlights 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 (Annelli, 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).

Bartnes and Moe (2017) Identified best practices for TTX to be successful: 1) define goals, 2) grow team knowledge, 3) invite all key personnel to participate, 4) create time pressure for quick decision-making, 5) use existing incident response plans, and 6) included management in the training exercise. Brilingaite et al. (2022) identified nine factors that can limit the effectiveness of information-sharing activities that should be addressed in training exercises. The nine factors are 1) a narrow focus on technical tasks, 2) required diverse technical skills, 3) no common vocabulary, 4) fragmented knowledge of legal documents, 5) missing knowledge of data exchange standards, 6) unfamiliarity with information-sharing platforms, 7) an excess of communication channels, 8) team size too small or too large, and 9) blurred benefits of skills outside the training exercise. The design of the scenario injections in the TTX is critical to achieving the desired outcomes (Lasky, 2010).

TTXs simulate a large-scale cybersecurity attack that is played out in a training setting to enable participants to gain knowledge and skills (Tobergte et al., 2022). TTXs should focus on communication, coordination and collaboration in response to the cybersecurity event (Vykopal et al., 2024). TTXs should improve participant awareness, provide education and training, and test participants' ability to detect and respond to a security incident in a coordinated manner (White et al., 2004). Exercises should improve both technical and nontechnical (e.g., problem-solving, communication, and teamwork) skills (Young & Farshadkhah, 2022). Critical infrastructure exercises should incorporate industry members, as well as city, state, and federal government agencies that would be involved in responding to a large-scale attack on critical infrastructure (White & Goles, 2004). Including government agencies in a critical infrastructure, TTX is an effective tool for building interagency networking, communication, and collaboration to respond to a large-scale security event(Sukhodolia, 2018). The scenario for an exercise must support the objectives and be realistic and relevant (Mäses et al., 2021). It should focus on people, process, and technology. The scenario should target organizational processes that are relevant to responding to cyber incidents.

**Cybersecurity Human Factors**

It is important to understand the impact of human factors on cybersecurity. Human factors are how humans interact with information technology, networks, and information security environments (Nobles, 2018). Many security breaches are the result of human error or mistakes in human decision-making (van Zadelhoff, 2016). Many of the human factors in cybersecurity are separate from traditional trait-based personality factors (Hadlington, 2018). For instance, security is affected by the humans involved in human-computer interactions (Nyre-Yu et al., 2019). Factors that might lead humans to take risky security actions include time pressure, workload, and an emphasis on working faster (Jalali et al., 2020; Nobles, 2018). Pollini et al. (2022) identified human security errors as 1) skill-based slips and lapses, 2) rule and knowledge-based mistakes, 3) intentional deviations from security policies, and 4) malicious violations intended to sabotage security policies.

Organizations need to develop human factor objectives in the information security strategy

(Nobles, 2018). This requires organizations to establish formal training and educational programs to address human factors in cybersecurity and to reduce security risk (Nifakos et al., 2021). To improve human factors in incident response, organizations must 1) conduct regular audits and risk assessments, 2) provide regular cybersecurity training, 3) establish clear communication channels, 4) foster a security-conscious organizational culture, and 5) implement regular updates and patches to address vulnerabilities (García, 2022). Conducting regular TTXs is a start to address human cybersecurity factors.

## 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 in the healthcare industry.

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 the Cybersecurity and Infrastructure Security Agency (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 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. 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. 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. All exercises had some participants in a face-to-face meeting room as well as others participating virtually via an internet videoconferencing system (Zoom).

## 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. This study will also analyze participant responses in TTX 1 to provide insight from the participants' perspective.

### 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 CISA coordinators, the National Guard, and 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 players from the power industry and 28 players 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. 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 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 15-minute large group discussion following each step of the TTX. During the 20-minute small group discussion, few players entered comments into the DECIDE platform. The content of the discussion was 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.

**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 was 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 of 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 on 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 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 discussions 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. A national CISA facilitator facilitated the session. 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 it 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.

## 4.ANALYSIS

The researchers developed an analytical method to examine the multiple data sources and developed summaries of the strengths and weaknesses of each TTX. The analysis used five aspects of the TTX (see Table 1): three inputs and two outcomes. The input categories were selected based on qualitative categorization. The outcomes were garnered from past TTX research, which argues 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 guarantee 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 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 the understanding of their strengths and weaknesses 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: A key to successful TTXs is the practice gained in incidents that require quick and effective collaboration. Effective collaboration involves exploring how to communicate efficiently with multiple stakeholders and understanding the necessity of having communication strategies in place before an incident takes place.

**Table 1: Evaluations of TTX**

| Aspect | TTX 1: Electrical Grid (State) | TTX 2: Electrical Grid (Regional) | TTX 3: Healthcare (Multi - Regional) |
|---|---|---|---|
| **INPUTS: Engagement** | • Small group - High engagement<br>• Virtual participants – lower engagement<br>• Issues with the DECIDE Platform. | • Participants - Knowledgeable and engaged<br>• Observers - limited participation<br>• Virtual participants - less active. | • Large group size limited individual participation. |
| **INPUTS: Facilitation** | • Small group - Effective facilitation<br>• Virtual participants - Challenges in managing engagement. | • Facilitators - led focused discussions effectively<br>• Facilitators - struggled to integrate virtual participants. | • Facilitator - Engaged state and federal experts effectively, virtual participants less active.<br>• Facilitator - Successfully involved experts and guided discussions. |
| **INPUTS: Technology** | • DECIDE Platform - Technical issues<br>• DECIDE Platform - Underutilized by some participants. | • DECIDE Platform - Better utilization compared to TTX 1<br>• DECIDE Platform - some technical issues. | • DECIDE Platform – Not Used; relied on traditional facilitation methods and physical presence. |
| **OUTCOME: Knowledge Gains** | • Participants - Gained knowledge on handling cyber incidents,<br>• Participants - Smaller cooperatives learning from larger companies. | • Increased knowledge and preparedness among participants with prior experience in cybersecurity exercises. | • Enhanced understanding of ransomware attacks<br>• Enhanced response strategies among healthcare providers with valuable input from state and federal experts. |
| **OUTCOME: Collaboration** | • Strengthened relationships<br>• Strengthened collaboration | • Effective collaboration among regional stakeholders.<br>• Limited observer participation. | • Improved communication<br>• 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 co-ops learned from the power company and vice versa because the co-ops 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 who were technically signed in to the Zoom session, but they didn't interact at all during the discussions.

In addition to evaluating inputs and outcomes, as shown in Table 1, the researchers analyzed participant responses to a series of questions posed by the DECIDE platform after each turn of the TTX to identify themes. Responses included comments on what went well and what did not go well. Responses were also analyzed to compare levels of participation by facilitators, observers, and players. Finally, the researchers conducted thematic analysis of the discussion summaries submitted by the observers of the nine groups after each turn in the exercise. The researchers used ChatGPT to do thematic analysis (Turobov et al., 2024). One of the researchers conducted member checking to validate the credibility of the results by doing a separate thematic analysis, which was compared to the ChatGPT thematic analysis.

Table 2 shows the thematic analysis of what went well, and Table 3 shows the thematic analysis for what did not go well. The themes for what went well were collaboration, networking and connection, grid and cyber knowledge, event organization, and virtual. Comments on collaboration included "Collaboration within small groups, State & Federal partners were introduced to Co-ops. Co-ops had the opportunity to meet one another." "The collaboration, and discussion topics were great, thought-provoking. I liked the scenario and cumulative impact." Comments for networking and connection were "Networking and making personal contacts that will be essential to be successful" and "Yes, very informative. A lot of information to take in at once though. Great to know what all services and aid is available for us as a utility!" A relevant grid knowledge comment was "The discussion periods with the various partners were great to get a better understanding of certain energy grid functions and responsibilities." Organization of the event was summarized by "Excellent preparation led to smooth experience for participants." A comment that summarizes the virtual theme was "The scenario wasn't specifically clear and was complex, like would probably happen in the real world. I was an online participant, and the breakout room worked well."

The themes for what did not go well were DECIDE, room & virtual setup, and time & information overload. Comments about DECIDE were "Trying to answer questions in the DECIDE platform and have meaningful discussion at the table is nearly impossible. I would consider leaving the DECIDE platform out of an in-person meeting. Although it is a great tool for online only meetings." And "DECIDE platform took significant time away from participating in the exercise. We could have covered much more information if we did not have to spend so much time on devices." The room & virtual setup comments were "There were only 2 to 3 of us in our chat room, I wish the group was a little bigger." Another comment was "Multiple room setup, hard to hear the other conversations." The comments for time and information overload were "A lot of info in short time. Hopefully I will retain it all." Another one was "A lot of information at once. For a non 'IT' person, several parts were hard to understand. Acronyms could be defined more during conversations."

**Table 2: What went well themes**

| Theme | Count | Frequency |
|---|---|---|
| Collaboration | 6 | 30% |
| Networking and Connection | 6 | 30% |
| Grid Knowledge | 4 | 20% |
| Organization of the event | 2 | 10% |
| Virtual | 2 | 10% |
| Totals | 20 | 100% |

**Table 3: What did not go well themes**

| Theme | Count | Frequency |
|---|---|---|
| DECIDE | 10 | 58.8% |
| Room & Virtual Setup | 4 | 23.5% |
| Time & Information overload | 3 | 17.6% |
| Totals | 17 | 100.0% |

This section looks at the level of participation in the DECIDE surveys after each turn of the TTX. Table 4 summarized the level of participation. There were four facilitators, 57 players, and 26 observers. The overall response rate by facilitators was 26.9%, for observer/scribes was 6.8%, and for players it was 44.7%. This supports the notion that there was a low percentage of use of the DECIDE platform. It is a valuable tool to support incident response exercises but was not used to its full potential in TTX 1. Part of the problem was DECIDE was used, Zoom was used between the rooms, and Zoom was used for the virtual participants. It was a complex exercise supported by several technical systems and the players prioritized participating in the face-to-face discussions over answering the survey questions in DECIDE. 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.

**Table 4: Participation in DECIDE Survey**

| Survey Section | Facilitator | Observer | Player | Totals |
|---|---|---|---|---|
| Onboarding survey | 2 | 11 | 39 | 52 |
| Sample Survey (Cyber) | 0 | 3 | 27 | 30 |
| Day 1 Questions | 2 | 3 | 31 | 36 |
| Day 2-6 Questions | 1 | 1 | 31 | 33 |
| Day 7 Questions | 3 | 2 | 33 | 38 |
| Day 8 Questions | 0 | 0 | 23 | 23 |
| Day 10-13 Questions | 1 | 1 | 23 | 25 |
| Day 15 Questions | 1 | 1 | 22 | 24 |
| Day 20 - 21 Questions | 0 | 0 | 21 | 21 |
| Day 22-23 Questions | 2 | 0 | 22 | 24 |
| Day 25 | 1 | 1 | 20 | 22 |
| Final Questions | 0 | 0 | 20 | 20 |
| Hotwash Survey | 1 | 0 | 19 | 20 |
| Average Responses | 1.1 | 1.8 | 25.5 | 28.3 |
| Total Participants | 4 | 26 | 57 | 87 |
| Response Rate | 26.9% | 6.8% | 44.7% | 32.5% |

The final analysis looked at the themes from the group discussions that were captured by the scribes that observed the nine groups during each injection of the TTX. The scribe notes were analyzed with ChatGPT using the prompt in the Turobov et al. (2024) journal article. One of the researchers went through the thematic codes that ChatGPT created and developed separate themes for member checking the ChatGPT results. ChatGPT created similar categorizations with the member checking, with some small differences. The researcher split out training and phishing into separate categories, while Chat GPT combined those two. With this difference removed, the percentages were roughly the same. The Chat-GPT groups of incident communication and management as well as social media and public communication fit well into the communication category. Perhaps the biggest discrepancy was the theme AI and cybersecurity tools in the ChatGPT analysis. AI was mentioned once or twice, but not sufficiently to serve as a theme name. The researcher lumped those under security preparedness. Finally, Chat-GPT either blindly categorized or ignored codes that fell under the "not useful" category. Regardless, ChatGPT did produce a classification quite close to the human researcher's classification. Table 5 shows the ChatGPT themes and Table 6 shows the researcher's themes.

Here is a list of the themes that the researcher came up with and a description of each. 1) Communications included comments about communicating within the organization, with media, or with law enforcement. 2) Internal threats had comments about dealing with the incident specifically. 3) Internal threats were about managing insider threats. 4) The not useful theme was missing information, comments lacking context, or too general for categorization. 5) Phishing was comments about dealing with phishing scams. 6) Security preparedness had comments about the need for pre-existing security protocols and processes. 7) Supply chain theme was comments about procuring technology, logistics, or threats to physical assets. And 7) training was comments about training employees to prevent or react to security events.

The researcher also served as a scribe observing group discussions during the TTX. The themes were similar to what the researcher observed during the exercise. Communications ranked as one of the most consistent themes of discussion. This represented the need for a known chain-of-command as well as having procedures for when to communicate outside the organization. Another common topic revolved around current security processes and potential changes to those processes to improve security. The final major topic is the "not useful" category. This category represents the fact that some comments lack sufficient context to be categorized. This represents one of the weaknesses of the DECIDE platform in that it relies on scribes to take down

pertinent information. This transcription can be hampered by multiple factors from familiarity with the DECIDE platform to the training of the scribe. As such, it can create inconsistent comments. Perhaps AI transcription would lessen or eliminate the problem for future exercises.

**Table 5: ChatGPT group discussion themes**

| Theme | Count | Frequency |
|---|---|---|
| Internal Threats | 3 | 7.7% |
| Phishing Prevention and Training | 5 | 12.8% |
| Incident Communication and Management | 7 | 17.9% |
| Collaboration and Mutual Aid | 6 | 15.4% |
| Supply Chain Challenges | 4 | 10.3% |
| Change Management | 3 | 7.7% |
| Social Media and Public Communication | 3 | 7.7% |
| AI and Cybersecurity Tools | 8 | 20.5% |
| Totals | 39 | 100.0% |

**Table 6: Researcher themes**

| Theme | Count | Frequency |
|---|---|---|
| Not Useful | 18 | 21.7% |
| Phishing | 4 | 4.8% |
| Communications | 20 | 24.1% |
| Incident Response | 4 | 4.8% |
| Security Preparedness | 24 | 28.9% |
| Training | 6 | 7.2% |
| Supply Chain | 5 | 6.0% |
| Internal Threats | 2 | 2.4% |
| Totals | 83 | 100.0% |

The virtual participants rarely interacted during the large group module summary discussions over Zoom. The virtual facilitator was also the scribe for the group and consequently had little time to submit summary comments after each turn of the TTX. All the comments from this group were related to problems with remote participation and the set-up of breakout rooms.

**Regional Electrical Grid TTX 2 Summary**

Like 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. TTX2 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. TTX2 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 was difficult for the face-to-face facilitator to actively lead a discussion between in-person and virtual participants.

**Healthcare TTX 3 Summary**

TTX3 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. TTX3 had over 100 participants both in the room and online. It was 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 during 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. TTX3 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 system as well as with the state and federal agencies that they would need to work with to recover from a ransomware attach 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.

## 5. CONCLUSION, BEST PRACTICES, & LIMITATIONS

This section discusses the best practices, limitations, and final conclusions. These recommendations should help academics and practitioners to lead effective critical infrastructure TTX exercises.

**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 communication 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 it 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 developing 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 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, the 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. 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 only TTX that had participant data to analyze was TTX 1. It would have been better to have the DECIDE data from TTX2, but it wasn't provided to the researchers. 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 the electrical grid and healthcare. The DECIDE platform that was used in two of the TTXs 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 and 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 a qualitative analysis of discussion transcripts from the exercises will help develop best practices by understanding the nuances of participant interactions and decision-making processes. This research analyzed the observer's comments and presented them in the TTX 1 summary. There was not a transcript of the verbal group discussions to analyze. 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).

**Conclusion**

In summary, tabletop exercises are an excellent choice to improve employee knowledge of cybersecurity risks in critical infrastructure. These case studies highlight the importance of active participation, skilled facilitation, and robust technology solutions to enhance the TTX experience. This study also emphasizes unique challenges in rural areas, such as limited resources. Further, this study highlights the need to explore the human element in cybersecurity to improve the resilience and security of critical fracture systems.

## 7.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

Annelli, 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

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

Berkeley, A. R., Wallace, M., & Coo, C. (2010). A framework for establishing critical infrastructure resilience goals. Final Report and Recommendations by the Council, National Infrastructure Advisory Council, 18–21.

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

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/ijsse.120304

Christiansen, J. (2022). How a well-thought-out incident response can take the advantage back from attackers. Cyber Security: A Peer-Reviewed Journal, 5(4), 316–323.

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

García, D. L. (2022). Human Factors in Cybersecurity Incident Response for Autonomous Vehicles - A Case Study Analysis: Examines human factors influencing cybersecurity incident response in AVs through case study analysis. Journal of Artificial Intelligence Research and Applications, 2(2), Article 2.

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

Hadlington, L. (2018). The "human factor" in cybersecurity: Exploring the accidental insider. In Psychological and behavioral examinations in cyber security (pp. 46–63). IGI Global. https://www.igi-global.com/chapter/the-human-factor-in-cybersecurity/199881

Jalali, M. S., Bruckes, M., Westmattelmann, D., & Schewe, G. (2020). Why Employees (Still) Click on Phishing Links: Investigation in Hospitals. Journal of Medical Internet Research, 22(1), e16775. https://doi.org/10.2196/16775

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

Lasky, M. (2010). The value of tabletop exercises and one-page planning documents. Journal of Business Continuity & Emergency Planning, 4(2), 132–141.

Malatji, M., Marnewick, A. L., & Von Solms, S. (2021). Cybersecurity capabilities for critical infrastructure resilience. Information & Computer Security, 30(2), 255–279. https://doi.org/10.1108/ICS-06-2021-0091

Mäses, S., Maennel, K., Toussaint, M., & Rosa, V. (2021). Success Factors for Designing a Cybersecurity Exercise on the Example of Incident Response. 2021 IEEE European Symposium on Security and Privacy

Workshops (EuroS&PW), 259–268. https://doi.org/10.1109/EuroSPW54576.2021.00033

National Cybersecurity Strategy. (2023). The White House. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. Sensors, 21(15), Article 15. https://doi.org/10.3390/s21155119

Nobles, C. (2018). Botching Human Factors in Cybersecurity in Business Organizations. HOLISTICA – Journal of Business and Public Administration, 9(3), 71–88. https://doi.org/10.2478/hjbpa-2018-0024

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

Nyre-Yu, M., Gutzwiller, R. S., & Caldwell, B. S. (2019). Observing Cyber Security Incident Response: Qualitative Themes From Field Research. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 63(1), 437–441. https://doi.org/10.1177/1071181319631016

Ota, Y., Mizuno, E., Aoyama, T., Hashimoto, Y., Koshijima, I., Asai, H., & Taniuchi, S. (2022). Designing Framework for Tabletop Exercise to Promote Resilience Against Cyber Attacks. In Y. Yamashita & M. Kano (Eds.), Computer Aided Chemical Engineering (Vol. 49, pp. 1471–1476). Elsevier. https://doi.org/10.1016/B978-0-323-85159-6.50245-1

Palleti, V. R., Adepu, 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

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: An integrated methodological approach. Cognition, Technology & Work, 24(2), 371–390. https://doi.org/10.1007/s10111-021-00683-y

Setola, R., De Porcellinis, S., & Sforna, 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

Sukhodolia, O. (2018). Training as a tool of fostering CIP concept implementation: Results of a table top exercise on critical energy infrastructure resilience. Information & Security: An International Journal, 40(2), 120–128. https://doi.org/10.11610/isij.4009

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

Turobov, A., Coyle, D., & Harding, V. (2024). Using ChatGPT for Thematic Analysis (arXiv:2405.08828). arXiv. https://doi.org/10.48550/arXiv.2405.08828

van Zadelhoff, M. (2016). The biggest cybersecurity threats are inside your company. Harvard Business Review, 19, 45.

Vykopal, J., Čeleda, P., Švábenský, V., Hofbauer, M., & Horák, M. (2024). Research and Practice of Delivering Tabletop Exercises. 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. 37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of The, 10 pp.

https://doi.org/10.1109/HICSS.2004.1265411

White, G., & Goles, T. (2004). The Role of Exercises in Training the Nation's Cyber First-Responders. New York.

Wrobel, L. A., & Wrobel, S. M. (2009). Disaster recovery planning for communications and critical infrastructure. Artech House.

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#page=4

## 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.

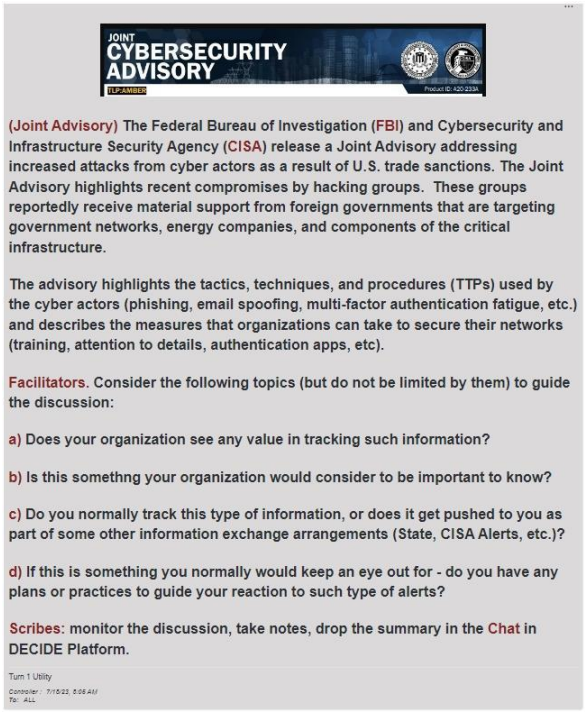
| Exercise Objectives | FEMA Core Capability |
|---|---|
| Establish a collaborative structure across county, city, and state utilities such that both communication coordination and investigation collaboration with outside agencies is open and aligned to build on one another's efforts and will avoid 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 Systems Cybersecurity |

| | |
|---|---|
| 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





- 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, 5:40 AM*
*To: NUARI (Observer), NUARI (Controller), Colorado Focal (Reviewer), Colorado Focal (Player), Colorado Focal (Observer)*

Turn 2: Scripted Response

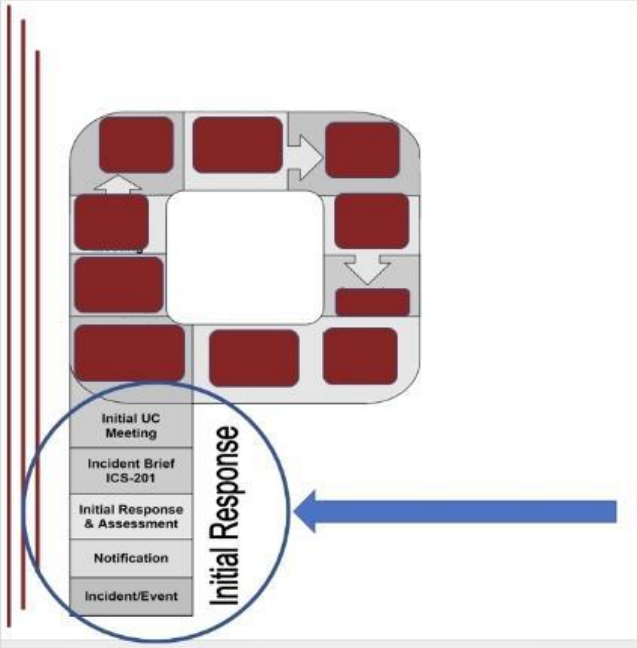
- Incident Response Plan (IRP) evaluation, application, and implementation

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? Wil 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 immediatelly 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?**

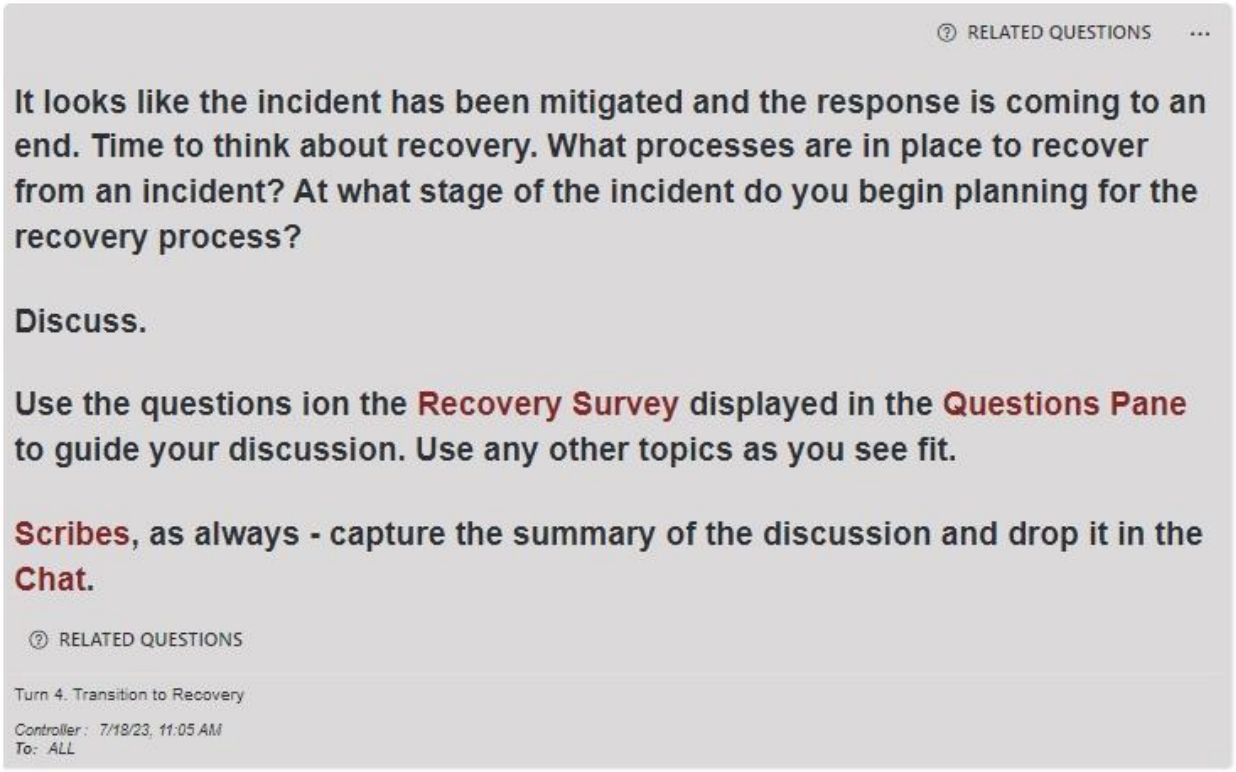
**Please follow the Mature Response Survey in the Questions Pane to use as guidance for the discussion, or feel free to use your own topics if they are more appropriate.**

**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




**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?

# PhishBusters: A Comprehensive Approach to Phishing Awareness Training in Organizational Settings

Melissa Montes
melissamontes@arizona.edu

Shengjie Xu
sjxu@arizona.edu

University of Arizona
Tucson, AZ 85721

## Abstract

This paper presents the design, implementation, and evaluation of PhishBusters, a comprehensive phishing awareness training program specifically developed for non-technical employees in organizational settings. The program employs a multi-faceted pedagogical approach that combines theoretical knowledge, hands-on exercises, and gamified learning to enhance participants' ability to identify and respond to phishing attempts. Through three structured training sessions, participants engage with realistic phishing simulations, interactive quizzes, and collaborative group discussions, fostering both individual skill development and peer learning. The effectiveness of the training program is demonstrated through comprehensive pre and post-assessment results, showing significant improvement in participants' ability to detect phishing attempts. The paper details the curriculum design process, implementation challenges, and participant feedback, providing practical insights into effective cybersecurity training methodologies. This case study contributes to the growing body of knowledge in cybersecurity education by demonstrating how well-designed training programs can successfully enhance organizational security awareness and reduce phishing susceptibility among non-technical staff.

**Keywords:**
Phishing awareness training, Cybersecurity education, Training program design, Employee security behavior, Interactive simulations, Organizational security training, Non-technical staff training

**Recommended Citation:** Montes, M., Xu, S., (2025). PhishBusters: A Comprehensive Approach to Phishing Awareness Training in Organizational Settings *Cybersecurity Pedagogy and Practice Journal;* v4(n2) pp 36-50. DOI# https://doi.org/10.62273/10.62273/JUZT9288

# PhishBusters: A Comprehensive Approach to Phishing Awareness Training in Organizational Settings

*Melissa Montes and Shengjie Xu*

## 1. INTRODUCTION

In today's fast-paced digital landscape, the security of an organization heavily depends on the awareness and vigilance of its employees. Cyber threats are evolving daily, and one of the most common and dangerous methods used by attackers is phishing (Verizon, 2023). Phishing is an attempt to steal sensitive information, typically in the form of usernames, passwords, credit card numbers, bank account information, or other important data, to utilize or sell the stolen information. By masquerading as a reputable source with an enticing request, such as an email or text message, an attacker lures the victim into giving up the information (Butavicius et al., 2022). Phishing attacks exploit human behavior, aiming to deceive individuals into divulging sensitive information and granting unauthorized access to systems.

The PhishBusters program was designed to empower employees at an organization who possessed little to no background in cybersecurity, by equipping them with the essential knowledge and skills necessary to effectively identify, avoid, and report phishing attempts. This comprehensive program immersed employees in a range of learning experiences that demystified the tactics employed by cybercriminals. Participants gained a deep understanding of how these threats manifest, allowing them to recognize suspicious emails, deceptive links, and fraudulent websites with confidence.

Through a series of engaging modules and interactive scenarios, employees gained not only the ability to spot red flags associated with phishing attempts but also the confidence to adopt proactive safety practices that significantly bolstered the protection of both their personal information and the organization's sensitive information. The curriculum was thoughtfully designed to cover a wide array of real-world examples of phishing attacks, delving into the various techniques employed by cybercriminals. This included the exploration of social engineering tactics, spear-phishing methods that target specific individuals, and the use of malicious attachments that can compromise systems.

Participants engaged in hands-on activities that simulated phishing attempts, allowing them to practice their skills in a safe environment. They learned how to scrutinize emails for suspicious elements, identify dubious links, and recognize fraudulent websites. Through group discussions, participants were encouraged to share their experiences and insights, fostering a collaborative learning atmosphere that enhanced their understanding of the topic.

By the end of the program, participants felt empowered and informed, equipped with practical tools and strategies to navigate the digital landscape securely. This newfound knowledge not only enhanced their personal cybersecurity practices but also cultivated a culture of vigilance and security awareness throughout the organization. As employees became more aware of potential threats that existed in their daily communications, they were more likely to report suspicious activities, contributing to a proactive security environment.

Ultimately, PhishBusters aimed to create a resilient workforce that stood united against cyber threats. By instilling a collective sense of responsibility and vigilance, the program helped safeguard the integrity of the organization and its valuable information, ensuring that all employees played an active role in protecting against cyber risk. Through this initiative, the organization enhanced its security posture, reduced the likelihood of successful phishing attacks, and fostered a culture of continuous improvement in cybersecurity awareness and practices.

## 2. LITERATURE REVIEW

### Why Phishing Works

Dhamija et al. (2006) aimed to address and test hypotheses on why users are most likely to fall for phishing attempts. Their study sought to understand the factors that contribute to users being deceived into falling for fraudulent websites. The goal of the Dhamija et al. study was to understand the reasons behind why phishing strategies work, in order to better learn from them and improve web browsers, websites, and other tools needed to protect users from phishing

attacks.

The Dhamija et al. study highlights gaps in user knowledge that phishing attacks exploit, such as lack of system knowledge and lack of security awareness. In terms of lack of system knowledge, many users do not understand how operating systems, browsers, and domain names work. Without this understanding, users have a difficult time recognizing phishing sites or forged email headers. In terms of lack of security awareness, users will often misunderstand security indicators like SSL padlock icons, which can be mimicked in webpage content. Users lack the proper skills to verify SSL certificates properly, making them vulnerable to spoofed trust seals and other deceptive tactics.

The Dhamija et al. study presents a usability study assessing how participants identify legitimate and phishing websites. Using 22 participants, the study analyzed their decision-making while interacting with real spoofed sites from financial and e-commerce companies. Factors such as website content, domain names, and security indicators were used to judge the legitimacy of a website. The results of the study found significant variability in users' ability to detect fraudulent websites, with some participants relying on visual cues while others used more advanced security knowledge. The study highlighted the challenges that even informed users face in recognizing phishing attempts.

From this study, the key takeaway that we can use to further develop our curriculum for this lesson is to consider that there are key factors often overlooked by those who are not technically inclined in technology. One must consider that simple factors, such as paying attention to the URL bar, can make a difference in showing whether a website is legitimate or spoofed. A basic understanding of indicators can go a long way in ensuring online user safety. If we provide focus and have participants learn and understand the common indicators that are a determining factor, we can make a difference in ensuring that participants are less likely to fall for phishing attempts.

**Does Phishing Training Work? Yes! Here's Proof**

Recent studies have shown that effective phishing training can significantly reduce employee susceptibility to phishing attacks (Goel et al., 2017). Phishing awareness training and phishing simulations are identified as the two main training approaches in this article (Moore and Clayton, 2007). The study aims to demonstrate how combining both training methods enhances the effectiveness of phishing training compared to using these methods separately.

Organizations that provide phishing awareness training report an 80% reduction in employee susceptibility after undergoing the training. This method aims to educate employees about the dangers of phishing threats, various attack types, and how to identify a phishing attempt in its tracks. Phishing simulations are tests that mimic real-world phishing scenarios, enabling employees to practice identifying potential threats. Research shows that simulation-based training can double learning retention, as employees have the ability to test their knowledge in real-life scenarios. By combining these two methods, organizations can see a 60% reduction in mistakes after a few sessions. The combination of both methods proves to be more effective than either method alone as it blends theory and practice, thus enhancing employees' readiness for real-world phishing attacks.

The article highlighted the importance of not only providing employees with proper phishing training but also the importance of incorporating phishing simulations, as these methods, when combined, prove to be effective together. These methods can provide insight into areas for improvement within their organization, helping them better prepare employees for the possibility of falling victim to such attacks. Our key takeaway from this article is that it will be in the best interest of participants to be provided with both types of training methods. In our setting, we will provide a phishing simulation email to employees before they receive any training. This will be followed by phishing awareness training, and then another simulation email to demonstrate the improvement that has taken place from going from no training to receiving training. By doing so, we will provide participants with hands-on experience in spotting phishing attempts and better instruct them on the common flags they need to be fully aware of.

**Phishing Detection: A Literature Survey**

Phishing targets the human factor as it is the weakest link in the security chain (Khonji et al., 2013). There is no single solution that can be deployed to address the issue, as phishing is a layered problem that must be addressed at two different levels: the technical and human layers. Solutions to address both layers can be found already, but it is unclear exactly how well they are working and whether they are making a difference today. There are currently two forms of

solutions employed: user education and software enhancement.

User education aims to increase awareness of phishing attacks and lower the risk of becoming a victim where software enhancements can be anything from apps to plugins to blacklist that provide support in stopping a phishing attack in its track.

The survey (Khonji et al., 2013) presents various phishing detection approaches, such as user education and awareness, Blacklists, Heuristic tests, and visual similarity, as well as machine learning-based classifiers, in which they test which approaches are best for dealing with phishing attempts. Their conclusions on the various approaches to combating phishing and enhancing end-user security are as follows:

- Education alone is insufficient because simply educating users about phishing risks is not enough. Even security experts can fall victim to phishing, suggesting that system complexities may exceed human cognitive limits. Hence, better system usability and user interfaces are crucial in addressing phishing risks. An example would be that active warnings (blocking content and visually signaling risks) are more effective than passive warnings.
- System behavior improvement can help mitigate phishing by automatically detecting and quarantining harmful messages through features like blacklists, heuristic rules, and machine learning techniques. These features are currently implemented in web browsers, email clients, and server-side filters.
- Blacklists are a list of previously detected phishing URLs, Internet Protocol addresses, and/or keywords, and are effective in reducing false positives. However, they struggle with mitigating zero-hour phishing attacks due to delays in detecting and updating the lists. Human-vetted blacklists, such as Phish Tank, have significant detection delays, leaving end-users vulnerable to new attacks during the early stage of a phishing campaign.
- Heuristic tests can detect zero-hour phishing attacks but tend to have higher false-positive rates than blacklights. The evolving nature of phishing tactics requires continuous updates to heuristic rules, making them expensive to maintain. Techniques that utilize visual similarity also incur computational overhead due to the rendering and analysis of web content, making them resource-intensive.
- Machine learning classifiers excel at addressing zero-hour phishing attacks and can automatically generate effective classification models from large datasets. They can achieve high accuracy, often with less than 1% false positives and over 99% true positives. ML classifiers can evolve over time, adapting to new phishing techniques without needing manual rule updates, making them more scalable and robust than heuristic-based approaches.

They concluded that while user education remains important, a more effective anti-phishing strategy involves a combination of systems usability improvements, blacklists, heuristics, and machine learning techniques to automate the detection and mitigation of phishing threats.

From their survey on different methods that can be used to prevent phishing attempts, our takeaway that we can use to further our program is to make it clear to employees that, in some cases, even with all the training in the world, not all phishing attacks can be prevented by being cautious. Some phishing attacks will be more sophisticated than others or be better hidden among legitimate emails. They will blend naturally and not raise any concern. In this case, ensuring that participants are well aware of risks that they may not be able to control and instead teach them to become aware and to communicate with the IT teams when it is deemed necessary. We can explore how advanced technologies such as machine learning, blacklists, and heuristic analysis contribute to mitigating phishing threats.

**Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions**

Sheng et al. (2010) evaluated different phishing educational materials to determine their effectiveness in training users. The materials tested included:

- Popular training materials include Microsoft Online Safety, OnGuardOnline phishing tips, and National Consumer League Fraud tips.
- Anti-Phishing Phil, which is an interactive game developed by Carnegie Mellon University (Sheng et al., 2007).
- Phish Guru Cartoon is a training system that uses cartoon images shown after users click on simulated phishing emails.
- Anti-Phish Phil with PhishGuru Cartoon, which is a combination of both training tools.

A total of 1001 participants were randomly assigned to different groups, including a control group (no training) and groups receiving one of

the training materials. Participants were given role-playing scenarios both before and after the training, and their reactions were analyzed to assess the impact of each tool.

The study found that all training approaches improved the true positive (TP) rate, meaning users were more likely to correctly identify phishing emails. However, most training materials also reduced the true negative (TN) rate, causing some users to distrust legitimate emails due to fear from their training. On average, training materials reduced false negatives (missed phishing emails) by 39.79% but reduced true negatives by 7.69%. Anti-Phish Phil stood out as the only tool that did not lower the TN rate, indicating it was more balanced in its approach. The control group (untrained) also showed slight improvement, as they received no training on how to identify or detect phishing attacks.

The study highlights that while user training can reduce phishing risks, it may also cause users to be overly cautious about legitimate emails. The effectiveness of training depends on balancing awareness without overwhelming users. Sheng et al. (2010) also provide further perspectives, noting that expecting users to become tech-savvy while handling their primary job tasks may hit cognitive limits. Meaning we cannot expect users with little technology background to become experts in the matter, IT needs to employ as many safeguards as possible to minimize the risk of phishing emails getting through the filtering system.

Participants with little background in technology can feel overwhelmed by the amount of information they need to learn to stay safe. For someone who is not used to seeing or learning about phishing, it can seem like a lot to take in, let alone memorize. For our program, we plan on teaching them some of the resources and tools they have available to them. The program is meant to be more engaging than others in hopes that they can retain information longer than learning on their own. By learning in a group setting, participants can learn from each other too and ask questions on the spot on anything that may need clarification. In doing so, the goal is for participants to walk away with knowledge that will help them change their behavior, thus changing their online habits for the better.

**Individual Processing of Phishing Emails: How Attention and Elaboration Protect Against Phishing**

Harrison et al. (2016) explores the idea of the mechanisms that influence susceptibility to phishing. They focus on the characteristics of emails, users' knowledge and experience with phishing (Williams et al., 2018). They conduct an experiment with 194 subjects in which they expose participants to phishing attacks to measure the participants' actions towards it. The goal is to reach an understanding that explains why some attacks are successful and why some participants are better at detecting phishing attempts (Parsons et al., 2013).

The study was done mainly on college students, as the younger population is often the most targeted of phishing attacks because of their low levels of phishing knowledge and awareness. Specially crafted emails were sent out to the participants, in which they had a fear-based and a reward-based email. The following hypotheses were tested:

- A fear-based phishing attack is more likely to result in decreased attention and decreased elaboration of the message than a reward-based attack. (H1a)
- A fear-based phishing attack is more likely to result in victimization than a reward-based attack. (H1B)
- The presence of leakage cues will result in increased attention and increased elaboration of the phishing message. (H2a)
- The presence of leakage cues will result in a lower likelihood of phishing victimization. (H2B)
- Increased subjective knowledge of and experience with email will lead to increased attention and increased elaboration of the phishing message. (H3a)
- Increased objective knowledge of and experience with phishing-specific emails will lead to increased attention and elaboration of the phishing message. (H3b)

The results were that 47% of participants clicked on the experimental link and provided their private information. Only 5% of participants noticed that the email did not come from a school domain, whereas 37% stated it did. The study determined that neither fear versus reward messaging nor the presence of leakage cues influenced the extent of the message elaboration, providing no support for H1a and H2a hypotheses. However, the subjective email knowledge, experience, and objective phishing-specific knowledge significantly predicted elaboration, supporting H3a and H3b. The overall model was significant; neither subjective nor objective knowledge alone was a strong predictor of elaboration.

For attention, message factors again did not impact processing, but objective phishing knowledge significantly improved attention, supporting H3b. The analysis revealed that both attention and elaboration were protective against phishing, with attention to specific elements such as hyperlinks or sender address predicting higher elaboration. However, the misinterpretation of certain cues, like perceiving a refund, reduced elaboration. Therefore, successful phishing defense involves recognizing key message cues and engaging in deeper message analysis.

The key takeaways from this study that we can use to further help our program will be to understand that, depending on one's experience, it will determine how well they can pick up on cues of a phishing attempt. Teaching participants that fear and reward-based tactics are common among phishing attempts, and it is in their best interests that they look at all the cues found in an email before they proceed to think irrationally and act on impulse. If we learn to take our time and read and analyze correctly, the chances of becoming a victim of a phishing attempt are low.

## 3. PROJECT DESIGN AND STRUCTURE

Using live lectures that are held in person, the phishing awareness training is split into three sessions to avoid an overwhelming amount of information at one time. Each session has participants learning the tools and skills that they need to ensure their online safety from any potential phishing attacks.

**Pre-Assessment**
The goal of designing a pre-assessment is to test the participants' current knowledge about the topic of phishing. It helps establish a baseline in understanding their familiarity with phishing concepts, risks, and detection techniques. This initial insight allows for a more targeted training that addresses the specific gaps or misconceptions. The pre-assessment was a crucial step in further developing lesson plans because it allows for:

- Identification of knowledge gaps: Helps uncover areas where participants lack essential understanding, enabling focus on topics where knowledge is weaker. In this case, the pre-assessment revealed that participants lacked an understanding of recognizing phishing indicators.
- Customization of Training: With a clear sense of participants' starting knowledge, the training can be tailored to be more effective, ensuring it is neither too basic nor too advanced for participants.
- Measurement of Progress: The assessment provides a benchmark to compare against the post-assessment, which helps measure the effectiveness of the training by showing how much participants have learned.

A simple ten-question multiple-choice survey was developed that asked participants to assess their current knowledge with regards to phishing. Participants were asked to complete the survey within two days of receiving the link to ensure enough time was given afterwards to analyze results and adjust lessons as needed. Out of the forty-two participants who took part in the survey, only seven respondents received a perfect score. The overall average score was 4.05 out of ten. The results were promising as they allowed for the identification of where common mistakes were occurring.

**Lecture Slides**
Three different slide decks were created to coincide with each lesson plan for the specific workshop. The slide decks are an essential part of the curriculum because they provide a structured, visual approach to learning, making complex information about phishing accessible and engaging. To avoid overwhelming participants with an endless amount of information, each slide deck was carefully planned and created in a visually appealing way, where the information on the deck was short and straightforward.

The first slide deck for lesson number one included introductory topics on what phishing, spear-phishing, whaling, smishing, vishing, and social engineering are. The common reasons why cybercriminals carry out phishing attacks, along with the type of information that they aim to steal. This presentation also included the methods used by attackers to target individuals, the dangers of such attacks, and a quick visual to illustrate how a phishing email works.

The second slide deck for lesson number two contained information regarding common indicators, how to verify an email address, what a domain is in email, hovering over links, malicious attachments, and how to identify suspicious links. Compared to the first slide deck, the second slide deck was made to be more interactive. After going over the topics, the next part added examples of simulations in which participants would be asked to first identify if the email was legitimate or a phishing email. From there, each participant would receive a chance to identify the indicators that they saw that made them determine whether or not an email was

legitimate.

The third and final slide deck contained a quick review of the first two sessions, along with topics that included:

- How to report phishing attempts to IT
- Steps to take if a malicious link is clicked
- Importance of multi-factor authentication
- Importance of strong passwords and password management

The purpose of this slide deck was to be more informative with information regarding how to mitigate and the tools at their disposal. The slide deck was not as interactive as the previous two, but it outlined important information to help change their online behaviors.

**Phishing Email Simulations**

Phishing simulations crafted in CanIPhish were a key part of the program to provide training to participants. These phishing simulations allowed for testing the participants' ability to identify and respond to phishing attacks without actual risk. A variety of emails were crafted to mimic the type of email an employee would be at risk of receiving daily. The phishing emails crafted displayed messages such as this person is trying to reach you via Teams, someone has shared a Dropbox file with you, reset password for Microsoft, the office Christmas party file has been shared with you, and the HR department is trying to share a file with you.

During the second session, participants used these emails crafted to identify the common red flags based on what they had just learned from the lecture slides. In doing so, participants had a better understanding of where exactly in an email would be signs of a phishing email, compared to just assuming. The simulations provided hands-on experience on the subject, which allowed for an interactive class in which they were taught and saw an example at the same time, which better served them to remember the indicators.

Before the first session of the program, along with the pre-assessment, participants were also sent a phishing simulation email to begin to test whether they would click on the link provided to them in the email in which it said they needed to update their password to a software application, however the link was malicious and instead collected their information and redirected them to a "ops, you've just been bait" message. After which the same email would be reviewed in session two and explained to participants, specifically those who clicked the email, on why it was a phishing email and what indicator was given in the email that was overlooked.

After the final session, participants would be sent another phishing email in hopes that all the information that they learned throughout the three sessions would benefit them in ensuring that they are able to identify the phishing email. The sole purpose of this final simulation email was to ensure that participants were able to properly identify common indicators, and in doing so it would allow for measuring the effectiveness of the program.

Phishing simulation emails are powerful tools for building resilience against phishing attacks. They give participants the practical, hands-on experience needed to recognize and avoid real-world phishing attempts, and ultimately help reduce the organization's vulnerability to these common attacks.

**Game Quiz using Kahoot**

Using Kahoot, an interactive quiz was made to be used during the live training to create an engaging learning environment while adding a bit of fun and competitiveness to empower employees to understand the topics. The game was designed to be used during the first session to review the topics and ensure participants understood what they had learned. It was created to test their new knowledge on the different types of phishing, the information they steal, and test their current knowledge of common red flag indicators, although this session would not touch on the subject.

**Infographics**

Using Canva, a quick and simple infographic was developed that participants could take with them and keep around their desk to refer to from time to time to refresh their memory on the subject, but also use when in doubt about an email. The infographic contains information about what cybercriminals are after, a quick definition of phishing, tips to help detect a phishing email, and what they can do to avoid falling victim to it.

**Post-Assessment Survey**

The last part in the structure of the program was to give out a post-assessment that would test participants on how well they remembered what they were taught. The post-assessment was sent out a week after the last session took place and was available to participants via Google Forms. The timeline for having results was the week of November 8, 2024, which gave time to compare results with the pre-assessment to determine whether the educational program was beneficial and find areas of improvement.

A final phishing simulation email was sent out as well that would truly test the knowledge retention of the participants to see if there had been improvement. The hope was to ensure that everyone who participated could differentiate legitimate emails versus fraudulent ones.

By the end of the course, participants understand common characteristics found in phishing attacks and the tools and skills to mitigate such a risk.

## 4. PILOT IMPLEMENTATION

The pilot of the program was given to the employees of a construction company. The program was given out in the span of two weeks, with almost every employee in attendance. Each live session was 45 minutes long in which included a period of lecture slides, examples, games, and questions/comments. Each of the live sessions included a group learning environment where participants were able to ask questions the moment they needed to and to encourage each other to do their best and learn the material. There were a total of 42 participants who took part in the PhishBusters training program, and the in-person training was held at an organization.

### Pre-Assessment and First Simulation Email

The first part of the program included sending out the pre-assessment survey and the first phishing simulation email to help the trainer have a better understanding of where the gaps in knowledge lie, to better help this group of participants. Once the results were received, the lessons were adjusted if needed to focus more on the gaps determined by the pre-assessments. In this case, most of the gap was in just understanding the common indicators, so a big focus was placed on ensuring that this topic was touched on, along with practicing it.

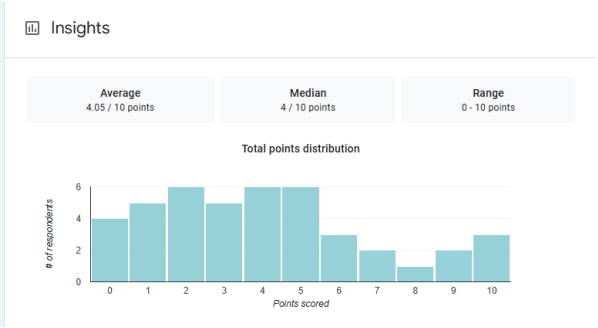



Figure 1: Pre-assessment results

The results of the pre-assessment in Fig. 1 showed that many of the participants understand what phishing is but fail to recognize common factors often used by cybercriminals. From the simulation email, over half of the participants actually inputted the credentials to change their passwords, hence falling victim to the simulated email. A quarter of the participants clicked on the link but never input their credentials, and the last bit of them discarded the email because some forgot, and the rest became suspicious of it. The results of the pre-assessment and the results of the simulation email helped pave the way for the pilot program to be implemented for a group of participants who showed a lack of understanding of the topic.

### Session One

In session one of PhishBusters, participants were introduced to the fundamentals of phishing, covering essential topics to build a solid foundation. The session began by exploring the several types of phishing attacks, including email phishing, spear-phishing, smishing, vishing, and whaling. Each type of attack was explained with examples to better help participants recognize how these tactics differ in approach and target.

The session then went on to discuss the reasoning behind phishing attacks, highlighting the motivation of cybercriminals, such as financial gain, data theft, and unauthorized access to systems. Participants learned about the types of information these attacks aim to steal, which can include login credentials, personal data, and financial information.

The session also emphasized the dangers of phishing attacks, underscoring the potential for financial loss, reputational damage, identity theft, and compromised security within organizations. Real-world examples were reviewed to illustrate the serious consequences of falling victim to phishing and the broad impact it can have on individuals and businesses alike.

To reinforce learning in a memorable way, the session ended with an interactive Kahoot quiz. The game reviewed the day's material, allowing participants to test their knowledge in a fun, competitive environment. This not only solidified key concepts but also created a lively and engaging conclusion to the session, setting a positive tone for the training journey ahead.

### Session Two

In session two of the PhishBusters, the focus was on building practical skills for recognizing phishing attempts, specifically in email form. The session began by discussing common indicators of phishing emails, such as suspicious sender

addresses, unexpected attachments, spelling and grammar errors, and urgent or threatening language designed to pressure the recipient into acting. The session covered how an attacker's main goal is to mess with their mind and act upon human behavior, in which one panics when receiving an alarming email instead of first stopping and thinking for a moment about where and why the email was coming.

Next, link-hovering techniques were introduced as a critical skill for phishing detection. Participants learned how to hover over links without clicking, revealing the actual URL and helping them verify the link's legitimacy. This led to exploring the concept of email domains with an emphasis on understanding how legitimate domains (like company URLs) differ from those commonly used in phishing attempts (such as a lookalike or slightly altered domains). The session then moved on to practicing identifying suspicious links, with participants examining examples to spot inconsistencies and subtle misspellings intended to trick users into trusting fake websites.

For hands-on practice, participants engaged with interactive slides where they reviewed simulated phishing emails to determine whether each one was legitimate or a phishing attempt. They were asked to highlight specific indicators that signaled a potential phishing email, helping them solidify their recognition skills in a controlled environment.

This session combined theoretical knowledge with practical exercises, empowering them to apply their training in real-world scenarios and boosting their confidence in identifying phishing emails accurately.

**Session Three**

In session three of PhishBusters, the session began by reviewing the key concepts covered in the first two sessions. The types of phishing attacks, common indicators, link-hovering techniques, and identifying suspicious domains were revisited, reinforcing participants' understanding and building confidence in their phishing detection skills.

After the review, participants were introduced to how to report phishing attempts within the organization, covering the steps for identifying and escalating suspicious emails. The session covered who the best person to contact is and the built-in reporting tools found in their email with a simple click. The importance of promptly reporting phishing attempts to reduce the organization risk and protect employees was emphasized.

The session discussed the proper steps to take if one does fall victim to clicking on a malicious link, including changing any compromised passwords, disconnecting from the network, and alerting the IT team so they can scan the system for any malware that may have been installed. It was an important topic to include in this session, as participants are left with an understanding of how to minimize potential damage if they were to fall victim to such an attack. Adding this topic to a phishing training program is important as not only do participants learn how to identify emails, but also what to do in case they mistakenly identify a fraudulent email as legitimate.

The session continued with a focus on multi-factor authentication (MFA) and password security. The importance of MFA as a defense mechanism that provides additional layers of security was covered, making it harder for attackers to gain unauthorized access even if credentials are compromised. Following that, strong password practices and password management tools were discussed, encouraging participants to create unique, complex passwords and use managers to securely store them.

The session concluded with a group discussion where participants shared their experiences, challenges, and thoughts on implementing these security practices in daily activities. This open forum allowed them to ask questions, exchange tips, and reinforce what they had learned in a collaborative environment, fostering a proactive approach to phishing prevention and cybersecurity awareness.

**Post-Assessment and Final Simulation Email**

In the post-assessment, participants completed a final evaluation to measure their knowledge retention and practical skills gained throughout the sessions. This assessment revisited key concepts covered in the program, including identifying phishing types, recognizing suspicious email indicators, and malicious links. The goal was to ensure that participants could confidently spot phishing attempts and respond correctly in real-world scenarios.

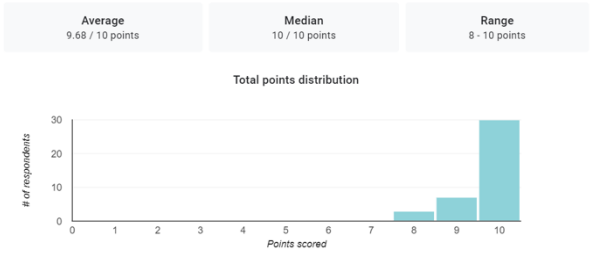



**Figure 2: Post-assessment results**

Fig. 2 shows the results of the post-assessment, where a significant jump in results from the pre-assessment can be seen. The results help give an insight into the success of the training, in which it can be seen that most participants increased their knowledge and understanding, and were able to accomplish significant improvement in identifying and understanding what phishing is.

Alongside the post-assessment, participants received a final phishing simulation email designed to test their ability to apply the training in a realistic situation. This simulation incorporated elements discussed in previous sessions, such as unusual sender addresses, subtle domain variations, and links to unverified websites. The hope was to ensure that the participants would use their newly acquired knowledge to ensure that they reported the email and did not act upon it. Successfully, all the participants were able to identify this email, and thirty-eight reported the email as phishing, and the rest deleted the email without clicking anything in it.

## Feedback Collection Methodology

To systematically gather participant feedback, we employed a multi-faceted approach that combined structured and informal feedback collection methods. This comprehensive approach allowed us to capture both quantitative and qualitative insights about the training program's effectiveness and participant experience.

### *Structured Feedback Collection*

We distributed a formal feedback survey to all 42 participants immediately following the completion of the third training session. The survey was administered through Google Forms and included both Likert-scale questions and open-ended response sections. The structured survey covered the following areas:

- Overall program satisfaction (1-5 scale)
- Clarity of content presentation (1-5 scale)
- Effectiveness of hands-on exercises (1-5 scale)
- Usefulness of phishing simulations (1-5 scale)
- Engagement level during group discussions (1-5 scale)
- Perceived improvement in phishing detection skills (1-5 scale)
- Open-ended questions about program strengths and areas for improvement

### *Informal Feedback Collection*

In addition to the structured survey, we conducted informal feedback sessions during and after each training session. These included:

- Real-time verbal feedback during group discussions
- Post-session informal conversations with participants
- Observations of participant engagement and interaction during activities
- Follow-up discussions with participants who had clicked on the initial phishing simulation

### *Feedback Analysis*

The feedback from the phishing program was overwhelmingly positive, with participants expressing high satisfaction across multiple areas that contributed to an enjoyable and effective learning experience. Everyone expressed their gratitude in terms that they felt the program was clear, effective, and easy to understand the concepts.

One of the main highlights was the clarity of the concepts presented. Participants consistently noted that the training content was broken down into easy-to-understand, digestible parts, making even complex aspects of phishing accessible to all skill levels. The straightforward explanations and clear examples helped demystify phishing tactics, enabling participants to grasp essential concepts quickly without feeling overwhelmed.

The hands-on practical exercises and realistic phishing simulations were another standout feature of the program. These exercises allowed participants to apply what they had learned immediately, giving them a chance to practice identifying phishing attempts in a controlled, real-world-like environment. Many participants commented that these simulations helped build confidence in recognizing phishing attempts and improved their skills in assessing suspicious emails and messages. This immersive approach not only reinforced theoretical knowledge but also equipped them with practical skills they felt ready to use in their daily routines.

Some of the participants also highlighted the

value of learning in a group environment. They found that collaborating with colleagues and discussing examples added an engaging, social dimension to the training. Working alongside others allowed for shared insights, encouraged discussions, and provided additional perspectives, making the learning process more dynamic and interactive. This environment also fostered a sense of teamwork and mutual support, further enhancing the experience.

Another popular element was the Kahoot quiz game that was incorporated after some of the lessons. This interactive quiz added a fun and competitive edge to the training, which helped lighten the learning atmosphere and made key takeaways memorable. By testing their knowledge in a playful format, participants could immediately see what they had retained, reinforcing core concepts while boosting their enthusiasm and engagement. The game also highlighted any remaining areas for improvement in a positive, low-pressure setting, which contributed to a lasting understanding of the material.

Overall, the training left participants feeling more confident and informed about phishing. They expressed appreciation for a well-rounded program that combined clarity, practical experience, interactive group work, and gamified learning to create a thorough and engaging educational experience.

## 5. REFLECTION

Reflecting on the PhishBusters program, the impact and positive feedback received from participants were extremely pleasing. Going into the training, the aim was to create a program that was accessible, engaging, and directly applicable to participants' everyday experiences with phishing. Seeing that participants found the material easy to understand confirmed that the right balance was struck in breaking down complex concepts into clear, straightforward explanations. Their comments on the clarity and accessibility of the content affirm that the efforts to demystify phishing terminology and methods were successful.

The hands-on practical exercises and simulations seemed to be a standout feature of the training, which was particularly rewarding to hear. These simulations were designed to bridge the gap between theory and real-world application, and participants' feedback suggests that they felt more confident in recognizing phishing attempts as a result. Watching them actively engage with these exercises reinforced the belief that practical experience is invaluable in cybersecurity training.

The group learning environment also played an impressive role. It was observed that it encouraged open discussions and knowledge sharing among participants. It was great to see how this setting fostered collaboration and allowed participants to learn from one another, making the training not only informative but also socially interactive. This added a level of engagement that contributed to the program's success, as participants felt supported and motivated by their peers.

The incorporation of the Kahoot game was a deliberate choice to make the training experience enjoyable and memorable. Based on feedback, the game's competitive yet lighthearted atmosphere achieved its purpose. It reinforced key concepts in a way that was both fun and effective, making the program feel less like a lecture and more like an interactive experience. Seeing participants eager to test their knowledge in this format confirmed the value of incorporating gamified learning into future sessions.

Participants' responses indicate that the program not only improved their phishing detection skills but also left them feeling more confident and empowered. This training reflection has reinforced the importance of balancing clarity, practicality, interactivity, and fun in cybersecurity education. Moving forward, these elements will continue to be refined to enhance engagement and effectiveness, knowing they resonate well and leave participants with a solid foundation to recognize and handle phishing threats confidently.

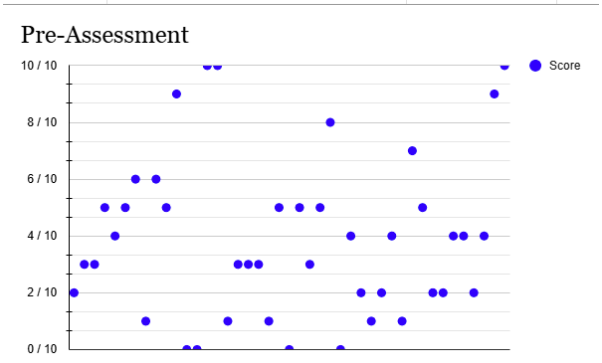



**Figure 3: Pre-Assessment Confidence Levels**

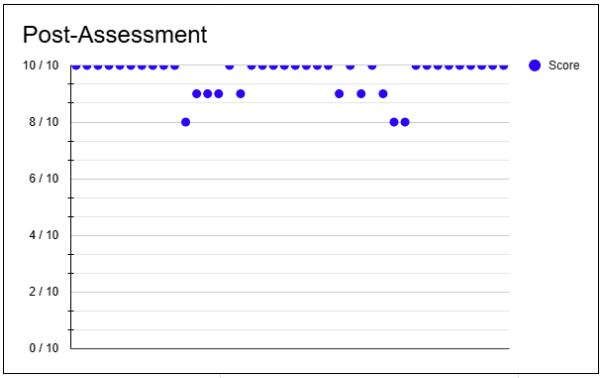



Figure 4: Post-Assessment Confidence Levels

The success of the program can be seen in comparing Fig. 3 and Fig. 4, which show the results of the pre-assessment scores and the post-assessment. An improvement can be seen where almost all participants scored significantly improved as compared to their first test scores. Analyzing the scores side by side allows for the conclusion that a vast majority of participants walked away with new understanding about phishing and have a better understanding of what it is and what they can do to protect sensitive information.

## 6. CHALLENGES

Developing a phishing training curriculum for employees with no prior knowledge of phishing presented several challenges that needed to be overcome to create a successful training program that would benefit everyone who participated in it.

**Simplifying Technical Concepts**
Phishing involves various technical elements such as domains, spoofing, and social engineering tactics that are difficult for non-technical participants to grasp. Having to simplify these concepts without oversimplifying or overwhelming participants is a challenge of its own, as one must figure out what information is key or a building block to ensure that participants will successfully understand the concepts at the end.

**Overcoming Initial Skepticism or Disinterest**
Participants unfamiliar with cybersecurity may not fully understand the relevance or importance of phishing prevention, which leads to disengagement. This makes it a crucial step to show them how phishing impacts them personally and professionally by showing them real-world examples or testimonies of victims who have lost so much by not being informed. This is a stepping stone in getting participants to want to participate and learn more about the topic.

**Building Confidence with New Skills**
For those participants with limited tech experience, actions like hovering over links or identifying email domain inconsistencies can feel intimidating. Ensuring they gain confidence and feel capable of using these skills requires a gradual, supportive approach with plenty of practice. Showing them and having them practice these skills while they are there ensures they can ask questions during the learning process, so when they are alone, they know exactly what to do and not to do.

**Avoiding Overload while Covering Essentials**
Participants new to phishing may begin to feel overwhelmed if there is too much information being presented at once. It is essential to prioritize key concepts and provide information incrementally, making it digestible and allowing time for practice. This was the main reason for splitting the training into three different sessions, in which each session covered different core concepts that serve as the foundation for understanding the topic.

**Creating Engaging and Relatable Examples**
Many phishing examples are built around IT-specific contexts. Finding examples that resonate with non-technical employees and relate to their everyday work and personal experiences is critical for engagement and retention. By creating examples that align with their work environment, an environment is created in which they see examples of what they may encounter in their everyday lives.

## 7. NEXT STEPS

After carefully analyzing the results of this training and considering the feedback received, several next steps and ideas have been identified to further refine the phishing training program.

**Enhance Realism in Simulations**
The introduction of more nuanced phishing simulations that mimic evolving tactics, including spear-phishing and whaling attacks, will help participants advance from basic to more sophisticated scenarios, building resilience against varied phishing techniques. Adding simulations that include smishing and social media-based phishing attempts will help broaden awareness beyond email-based phishing and reinforce cross-platform vigilance.

**Expand Hands-On Practical Components**

Beyond incorporating phishing exercises during the training, providing "surprise" phishing emails throughout the training can help test participants' skills at random points and see how vigilant they are. A module could also be added where participants simulate reporting a phishing attack, documenting it, and following an incident response plan. This step could help reinforce proper response protocols and ensure participants know what to do when they spot a potential threat.

**Increase Personalized Feedback and Follow-up**
Personalized feedback can be provided after each phishing simulation, focusing on what participants did well and areas where they can improve. This will encourage continuous learning and allow individuals to refine their skills in real time. The introduction of quarterly phishing simulations as ongoing training, with reports that track improvements and highlight recurring issues, would create a continuous learning loop and help reinforce the knowledge gained in the initial training.

**Introduce Gamification and Interactive Learning Modules**
In addition to Kahoot, other quiz formats or gamified challenges (like scenario-based role-playing games) could be considered, where participants decide how to respond to a potential phishing email in different contexts. A leaderboard through the program could be implemented that recognizes top performers in phishing simulations or quizzes. This could foster friendly competition and motivate participants to stay engaged and alert.

**Leverage Peer Learning and Group Exercises**
Opportunities could be created for participants to analyze real phishing cases in small groups, encouraging discussion on what tactics were used and how they could be detected. This could also be used as an ongoing activity that keeps teams informed of new phishing techniques. Another option could be to pair participants with a "security buddy" to encourage collaboration, allowing them to check in with each other on suspicious emails or share insights, fostering a culture of teamwork and continuous learning.

**Expand the Scope of Training with Specialized Modules**
PhishBusters could develop specialized modules tailored to specific roles, such as finance or HR, which often face unique phishing risks. Customizing content to match participants' job functions will improve the relevance and applicability of the training. Optional modules on advanced phishing tactics (like email spoofing and social engineering) could be provided for those participants who may require a deeper understanding of these issues.

**Gather Long-Term Feedback and Track Progress**
Follow-up surveys and periodic knowledge assessments could be implemented to track how well participants retain the material over time, allowing adjustments based on the latest trends or areas of improvement. The data collected could be used to identify trends such as common mistakes or departments with higher click rates, to tailor future training and reinforce high-risk areas.

By building on these next steps, the phishing training can become an even more comprehensive, practical, and engaging program, promoting continuous improvement in phishing awareness and response across the organization. In the future, the possibility of implementing a program like this one at the high school level when teenagers are using technology a lot more could be explored to ensure phishing education begins early on in their lives.

## 8. CONCLUSION

In conclusion, the PhishBusters training program has proven to be a valuable and well-received initiative, effectively enhancing participants' phishing awareness and response skills. Feedback has highlighted the program's clarity, hands-on exercises, and engaging group environment, as well as the success of interactive elements like the Kahoot game, which made learning enjoyable and memorable. Reflecting on the training experience, it is clear that combining straightforward explanations, practical simulations, and gamified learning can significantly enhance confidence and knowledge in phishing detection, particularly for individuals with diverse skill levels.

Looking ahead, there are many promising opportunities to further refine the program. By increasing simulation complexity, expanding role-specific training, and incorporating ongoing assessments and feedback, it can be ensured that PhishBusters training remains relevant, practical, and effective. Adding quarterly simulations, leaderboards, and real-life case discussions will keep participants engaged and vigilant, fostering a culture of continuous learning. Altogether, these steps will not only improve phishing recognition skills but also support a proactive and

security-minded organization well-pared to handle evolving phishing threats.

By creating PhishBusters, employees were empowered with the knowledge and skills to recognize and respond to phishing threats. A proactive security culture was fostered that reduces the likelihood of successful phishing attacks and mitigates potential organizational risks. By educating employees on phishing tactics, prevention strategies, and response protocols, their confidence and vigilance were enhanced, making them the first line of defense against cyber threats. Additionally, by incorporating engaging and practical elements like simulations and group activities, the training was made impactful and memorable, leading to long-term behavioral change and a more resilient organization overall.

## 9. REFERENCES

Marcus Butavicius, Ronald Taib, and Sigi J. Han. Why people keep falling for phishing scams: The effects of time pressure and deception cues on the detection of phishing emails. *Computers & Security*, 123: 102937, 2022. doi: 10.1016/j.cose.2022.102937. URL https://doi.org/10.1016/j.cose.2022.102937.

Rachna Dhamija, J. Doug Tygar, and Marti Hearst. Why phishing works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 581–590, New York, NY, 2006. Association for Computing Machinery. doi: 10.1145/1124772.1124861. URL https://doi.org/10.1145/1124772.1124861.

Sanjay Goel, Kevin Williams, and Ersin Dincelli. Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems*, 18(1):2, 2017. doi:10.17705/1jais.00447. URL https://doi.org/10.17705/1jais.00447.

Brian Harrison, Elena Svetieva, and Arun Vishwanath. Individual processing of phishing emails: How attention and elaboration protect against phishing. *Online Information Review*, 40(2):265–281, 2016. doi: 10.1108/OIR-04-2015-0116. URL https://doi.org/10.1108/OIR-04-2015-0116.

Mahmoud Khonji, Youssef Iraqi, and Andrew Jones. Phishing detection: a literature survey. *IEEE Communications Surveys & Tutorials*, 15(4):2091–2121, 2013. doi: 10.1109/SURV.2013.032213.00009. URL https://doi.org/10.1109/SURV.2013.032213.00009.

Tyler Moore and Richard Clayton. Examining the impact of website take-down on phishing. In *Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit*, pages 1–13, New York, NY, 2007. Association for Computing Machinery. doi: 10.1145/1298955.1298956. URL https://doi.org/10.1145/1298955.1298956.

Kathryn Parsons, Agata McCormac, Marcus Pattinson, Marcus Butavicius, and Cate Jerram. Phishing for the truth: A scenario-based experiment of users' behavioural response to emails. In *Security and Privacy Protection in Information Processing Systems: 28th IFIP TC 11 International Conference, SEC 2013*, pages 366–378, Berlin, Heidelberg, 2013. Springer. doi: 10.1007/978-3-642-39345-7_39. URL https://doi.org/10.1007/978-3-642-39345-7_39.

Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd Symposium on Usable Privacy and Security*, pages 88–99, New York, NY, 2007. Association for Computing Machinery. doi: 10.1145/1280680.1280692. URL https://doi.org/10.1145/1280680.1280692.

Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Julie Downs. Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 373–382, New York, NY, 2010. Association for Computing Machinery. doi: 10.1145/1753326.1753383. URL https://doi.org/10.1145/1753326.1753383.

Verizon. 2023 data breach investigations report. Verizon Business, 2023. URL https://www.verizon.com/business/resources/reports/dbir/. Retrieved from https://www.verizon.com/business/resources/reports/dbir/.

Emma J. Williams, Joanne Hinds, and Adam N.

Joinson. Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, 120:1–13, 2018. doi: 10.1016/j.ijhcs.2018.07.003. URL https://doi.org/10.1016/j.ijhcs.2018.07.003.

*Teaching Case*

# Utilizing a Virtual Firewall Appliance for Introducing and Reinforcing the Concepts and Implementation of Devices to Improve Security in a Computing Environment

Stanley J. Mierzwa
smierzwa@kean.edu

Christopher Eng
engchr@kean.edu

Center for Cybersecurity
Kean University
Union, NJ 07083, USA

## Abstract

As cybersecurity education in higher education continues to evolve, there is a growing emphasis on experiential learning and practical skill development aligned with real-world work roles. Programs designated as National Security Agency Centers of Academic Excellence increasingly require students to demonstrate advanced competencies across a range of cybersecurity domains. Among these, firewall technologies remain foundational to network and information security practices. This paper presents a classroom implementation project that integrates a commercially available virtual firewall into an introductory cybersecurity course. The goal was to provide students with an authentic, hands-on experience in configuring and managing firewall systems. The paper outlines the instructional design, tools used, and step-by-step implementation process, offering a replicable model for faculty interested in incorporating similar activities into their curriculum. Additionally, student feedback collected through a post-activity survey is analyzed to assess the effectiveness of the virtual firewall experience in enhancing learning outcomes. The results suggest that virtual firewalls can serve as a valuable pedagogical tool in cybersecurity education, bridging theoretical concepts with practical application.

**Keywords:** Pedagogy; Firewalls; Virtual Machines; Cybersecurity; Hands on Learning

**Recommended Citation:** Mierzwa, S.J., Eng, C., (2025). Utilizing a Virtual Firewall Appliance for Introducing and Reinforcing the Concepts and Implementation of Devices to Improve Security in a Computing Environment *Cybersecurity Pedagogy and Practice Journal;* v4(n2) pp 51-66. DOI# https://doi.org/10.62273/BEOJ9082

# Utilizing a Virtual Firewall Appliance for Introducing and Reinforcing the Concepts and Implementation of Devices to Improve Security in a Computing Environment

Stanley J. Mierzwa and Christopher Eng

## 1. INTRODUCTION

This activity provided an opportunity to explore the feasibility and practical case study of using a virtual firewall configuration that was co-designed as a form of teaching pedagogy to provide a real-world connection between professional firewall devices and students. The design was created and pursued between a National Security Agency Center of Academic Excellence in Cyber Defense designated program and an industry provider of cybersecurity tools and technologies, including firewalls, endpoint security devices, intrusion detection, and artificial intelligence capabilities integration. One critical motivation for tackling this effort was to allow students in a cross-disciplinary undergraduate firewall course access to more hands-on experience in using a professional firewall. Additionally, a motivation was to include a student worker from the university's information technology department in the opportunity to partner with a faculty member on this activity. Finally, the inspiration also sought to document the solution in the event that other educators wished to explore the solution utilized.

Content is provided outlining the theoretical framework and model utilized as a guide in this activity, as well as background information on the said course that introduced a virtual machine firewall. Additionally, background information is provided on the technology and foundational settings utilized to make the solution available. Finally, a discussion is provided outlining the feedback assessed from students, activities to pursue going forward, and other implications.

## 2. THEORETICAL MODEL AND FRAMEWORK

As a theoretical guide to this effort, the instance-based learning theory was employed as a framework. Instance-based learning theory (IBLT) has been employed in previous cybersecurity research to explain situational awareness and provide models for acquiring real-world cybersecurity domain knowledge and experience (Veksler et al., 2018). Instance-based learning theory provides the theoretical background focused on the premise that every decision in a situation can be referenced back to an experience, known as the instance (Dutt et al., 2013). The theory provides a framework to follow in order to attempt to predict activities and timing based on threats through cybersecurity situational awareness (Gonzalez et al., 2003). In this activity, the ability to interface with virtual firewalls, given sequences and scenarios to follow, was approached and aligned with the IBLT by allowing the students to navigate the firewall in the same manner as professionals in the field. A train-the-trainer activity took place with a Fortinet engineer providing in-person instruction on the firewall solution, utilizing the materials that could be used for laboratory experiences (Fortinet, 2024). This action was meant to frame the purpose and reasons one would configure or reconfigure and program a virtual firewall, as well as create a reference point. As an example, a reference point outlined included the acquisition of a firewall, determining if any rules and configurations were to be migrated over to the new device, as well as the initial setup that was detailed for the students to pursue in a vendor-supplied laboratory exercise.

## 3. FIREWALLS SPECIFIC COURSE

### Rapid Literature Review

In its most basic functionality, a firewall is a technological solution that is implemented to secure the perimeter of networks against unwanted breaches and cyber-attacks (Haghighi et al., 2024). In the field of information security, a firewall solution is often implemented by an expert who has experience in creating rules that allow or disallow specific types of network traffic. Network traffic can be filtered between operating zones by using a firewall. The detection and ability to block attacks via Intrusion Detection and Intrusion Prevention Systems (IDS/IPS) are often features built into a firewall device (Hassan, 2020).

Prior to introducing the use of virtual firewalls as part of a pedagogical strategy for a course, several steps were taken to conduct a rapid literature review. These steps included performing focused searches in several scholarly

databases and repositories. The result of this rapid literature review activity yielded a lack of such documented materials. The search criteria utilized within the demonstrated databases included performing a full-text search at any time and using the focused search terms of pedagogy with the Boolean AND operator and "virtual firewall." The goal of such a search was to quickly glean if other researchers and practitioners have put forth an effort to document the use of virtual firewall solutions, regardless of make, model, vendor, and strategies within the scholarly literature. The results are outlined in Table 1.

Using other novel techniques can be helpful in bringing forward a positive pedagogical method to instill knowledge and background on firewall technologies. Rozinaj et al. (2018) utilized the self-directed learning method with the use of virtual reality and the use of games to engage firewall technology knowledge users of the solution. Gampell et al. (2024) partnered with students, academics, and emergency management professionals to create a pedagogy that supported the use of a gaming platform that engaged students in learning about disaster critical adverse events risk reduction.

The role of firewalls extends to many different computing environments, including those that can be associated with the Internet of Things (IoT), which can be included in such areas as manufacturing. Previous research into the use of Palo Alto firewalls and their integration with IoT was approached as a form of pedagogy to understand such real-world scenarios (Sanchez et al., 2020). Many different firewall vendors provided solutions exist, and in the next section, an outline of the tasks that led to the product utilized in this pedagogical activity.

| Database or Source | Search Term | Number of Entries |
|---|---|---|
| Google Scholar | "pedagogy" and "virtual firewall" | 37 |
| ACM Digital Library | "pedagogy" and "virtual firewall" | 4 |
| IEEE/IET Electronic Library | "pedagogy" and "virtual firewall" | 0 |
| EBSCOhost | "pedagogy" and "virtual firewall" | 0 |
| ABI/INFORM Global | "pedagogy" and "virtual firewall" | 2 |
| Homeland Security Digital Library | "pedagogy" and "virtual firewall" | 0 |

**Table 1: Academic Literature Rapid Scan**

**Course Details and Student Population**

The cross-disciplinary course is titled Firewalls and Secure CPU (CJ3760). It is available to students pursuing a Bachelor of Science in Computer Science with a Cybersecurity option, a Bachelor of Science in Information Technology with a Cybersecurity option, and a Bachelor of Arts in Criminal Justice with a Cybersecurity concentration. Prerequisites to take CJ3760 include completion of an introductory cybersecurity course named Foundations in Cybersecurity (CJ2630). The prerequisite CJ2630 course includes theoretical content covering a broad set of topics, including an overview of cybersecurity, cybercrime, and the Internet, hacking, intellectual property, scams and fraud, online victimization of individuals, policing the Internet, cyber liberties, and the future of cybercrime and information security. The firewall course has traditionally been given from a theoretical perspective, with limited laboratory exercises, following the guidelines and curriculum outlined in a book published by Pearson. The course is given to students who have taken prerequisite information technology, computer science, or cybersecurity coursework but is considered an introduction to the concept, functionality, and implementation of firewalls to secure computing environments. The course is basically broken up into a 16-week program, with eight weeks focused on firewalls and eight weeks dedicated to securing computing environments, such as workstations, PCs, and other endpoints, via technical group policies and procedures. It is expected to have students from a variety of disciplines of computer science, information technology, and criminal justice. An example of several of the starting point laboratory exercises are presented in Appendix A and B.

## 4. METHODS

**Partnering with a Firewall Vendor**

A variety of professional vendor options, in the form of software and hardware, exist for computer networks, servers, workstations, routers, access points, and the like for an enterprise computing operation. A good number of options exist for firewall devices. The devices

can exist in hardware-based appliances with integrated hardware and software or the use of virtual software options to employ on one's hardware platform or virtual server configuration. In the case of this academic activity, to provide students with the ability to engage with a real-world vendor firewall, several vendors were contacted to inquire about the potential for an open educational resource or freely available options for students. An important aspect was to minimize the costs for students to operate firewalls in a laboratory environment. One vendor was rapid to the table with options, Fortinet. There could have been more vendor-based solutions and freely available options. However, Fortinet provided excellent input and guidance and was willing to visit the campus for a full day to both present and work on the established setup and configuration, and provide example labs that could be implemented.

The laboratory hardware components utilized for the firewalls course included the use of standard Windows 10 laptops, having the latest software and security updates, the freely available Oracle VM VirtualBox Manager (version 7.0.14 r161095), and the Fortinet FortiGate VM for VMWare. It was decided to use the available course laptops to minimize the solution requirement constraints since some students use Google Chromebooks, which would cause challenges for the installation and setup. The requirements to run VirtualBox include the use of either an Intel or AMD processor, ample RAM, depending on the operating system one wishes to run, and large enough disk space to host the virtual machine desired (Oracle VirtualBox, 2024). For the specific FortiGate VM used in the lab exercises, a base memory of 5 GB was enabled, along with 8 to 10 GB of disk space. For the virtual provisioning of the CPU, the setting of 4 Cores was configured. The exact image utilized for this case study was named FGT_VM64_HV-v7.4.2.F-build2571-FORTINET. The virtual image for the Fortinet FortiGate can be found by navigating and registering at the FortiGate Cloud web portal (https://www.forticloud.com). In the laboratory scenario utilized in this effort, the product image selected was the FortiGate product for Hyper-V to operate in a Windows Operating System environment.

The laptops are required to be connected to a wired or Wi-Fi network connection with Internet connectivity available in order to register the demonstration version of the virtual firewall. In order to permit the Fortinet FortiGate VM firewall to communicate with the local area network and the Internet, a vital adjustment was necessary. The network setting of the Oracle VM VirtualBox image mounted required the enabling of the network-bridged adapter setting. These settings can be seen in Figure 1.

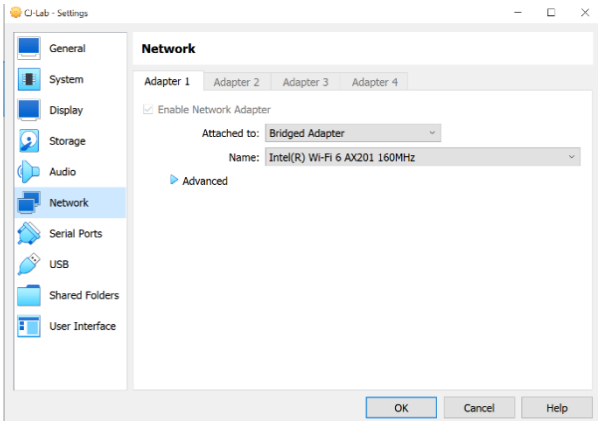



**Figure 1: VirtualBox Bridged Adapter**

**Firewall Configuration and Settings**

Upon starting up the Fortinet FortiGate firewall within the VirtualBox manager, the student is confronted with a pure command-line interface. Using a command line interface to configure a firewall provides students with a valuable and realistic knowledge and skills activity. By providing students a task to execute command line functions, they have the opportunity to recognize that firewalls can be configured by using a web interface as well as a traditional command line. A sample screen with the high-level configuration options made available by simply entering "?" is provided in Figure 2. Students were then asked to review all the high-level options available to them when using the command line interface.

```
FGVMEVRMOIQKX9BC login: admin
Password:
Welcome!

FGVMEVRMOIQKX9BC #
config       Configure object.
get          Get dynamic and system information.
show         Show configuration.
diagnose     Diagnose facility.
execute      Execute static commands.
alias        Execute alias commands.
exit         Exit the CLI.

FGVMEVRMOIQKX9BC #
```

**Figure 2: Command Line Help Interface to Firewall Settings and Configuration**

**Initial Assignments and Lab Activities**

In addition to providing the setup and installation instructions in order to get the virtual firewalls up and running, students were asked to follow and respond to prompts of growing complexity in navigating the firewall. Greater confidence in getting started with the configuration of a network perimeter defense device provides an

anchor or initiation step that helps one get oriented. Initial steps included logging into the command prompt interface, executing a ping to ensure proper connectivity existed, and proceeding through the steps to obtain the IP address assigned to the firewall. In addition, verifying the DNS settings and ensuring there is the ability to access public websites outside the laboratory environment was possible. The screen examples students would use with these successful steps can be found in Figures 3 and 4.

```
FGVMEVRMOIQKX9BC # execute ping www.yahoo.com
PING me-ycpi-cf-www.g06.yahoodns.net (69.147.92.11): 56 data bytes
64 bytes from 69.147.92.11: icmp_seq=0 ttl=51 time=11.7 ms
64 bytes from 69.147.92.11: icmp_seq=1 ttl=51 time=10.0 ms
64 bytes from 69.147.92.11: icmp_seq=2 ttl=51 time=26.4 ms
64 bytes from 69.147.92.11: icmp_seq=3 ttl=51 time=11.9 ms
64 bytes from 69.147.92.11: icmp_seq=4 ttl=51 time=10.4 ms

--- me-ycpi-cf-www.g06.yahoodns.net ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 10.0/14.0/26.4 ms
```

**Figure 3: Executing a Command Line Connectivity Test**

```
FGVMEVRMOIQKX9BC # diag ip addr list
IP=10.140.35.85->10.140.35.85/255.255.240.0 index=3 devname=port1
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=5 devname=root
IP=10.255.1.1->10.255.1.1/255.255.255.0 index=9 devname=fortilink
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=10 devname=vsys_ha
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=12 devname=vsys_fgfm

FGVMEVRMOIQKX9BC #
```

**Figure 4: Obtaining IP Address from the Command Line**

After struggling a lot with a command line interface, it was then time to provide students with the steps and procedures to access the graphical user interface, which is made available via an HTTPS page. The challenges with the command line interface included ensuring that commands were executed with proper syntax and with passing parameters. This was a new concept for some of the students who did not have a deep technical academic background, for example, those pursuing criminal justice degrees. Understanding the concept of getting started with a firewall configuration with a command line is a critical competency to develop since the practice can translate to other appliance devices, such as network switches. Students were instructed to utilize the private IP address obtained in an earlier lab to bring up the HTTPS interface in a browser. The login prompt provided in the browser, if successfully rendered, and the initial Fortinet FortiGate dashboard pages can be seen in Figures 5 and 6. The dashboard provided the students the opportunity to witness the web interface utilized to configure a firewall and monitor its activity.

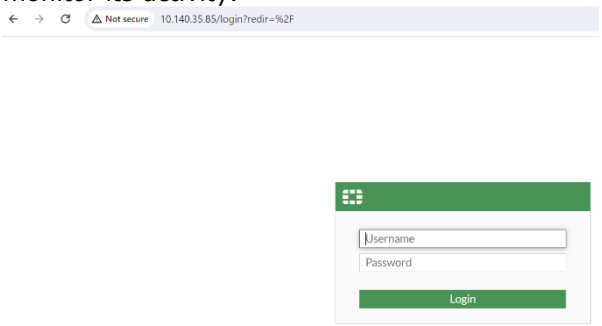



**Figure 5: Firewall HTTPS Interface Login**

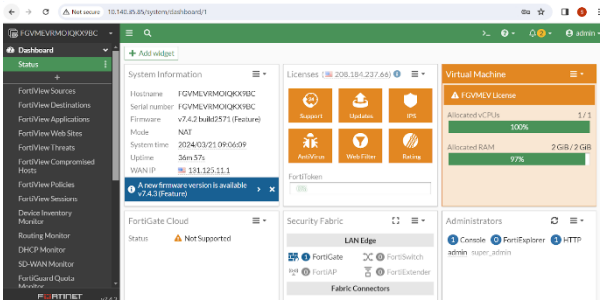



**Figure 6: Virtual Firewall HTTPS Dashboard**

## 5. RESULTS

The field of cybersecurity, including the technology and solutions that can be implemented, as well as the practices and procedures to consider, is vast. Providing students with more interactive and hands-on activities is beneficial in understanding the many building blocks required to secure an organization and computing environment. The pedagogy involved in instructing students on content related to firewalls will be beneficial in building more excellent competencies with the introduction of a "real-world" firewall device with which to engage. In addition to a critical theory, firewalls are a specific product set solution. They are still considered standard devices for implementation in any company, business, agency, or organization that connects to the public Internet. In fact, many organizations employ and have implemented many firewalls within their infrastructure in order to create separate networks with greater granular control. The use of a set of laboratory exercises to complement seeing a firewall first-hand can be beneficial to a recent cybersecurity graduate entering the field.

## 6. DISCUSSION AND IMPLICATIONS

The feedback survey results from students who utilized the firewall virtual machine configuration

outlined in this document found it to be meaningful. Every student in the course reported that this was their first time engaging, navigating, and configuring a firewall security appliance and device. All students (*N*=14) reported that the complement of using a virtual firewall device improved their understanding of how such devices can be used in businesses and organizations to protect the environment. Improving and enabling greater competency was reported as achieved. An open question was administered to obtain further suggestions for improvements in future classes. A common theme suggested was to engage even further with more laboratory time to allow for greater self-learning and optional laboratory assignments. The self-report web-based Google Forms surveys were administered to all the students in this introductory firewall course at the end of the course, as well as laboratory exercises.

## 7. CONCLUSION

Cybersecurity education at both undergraduate and graduate levels benefits from diverse pedagogical approaches that blend theory with practice. This paper demonstrated how integrating virtual machine firewalls into coursework can significantly enhance students' practical understanding of network security technologies. By moving beyond theoretical analysis, students engage directly with real-world tools, gaining hands-on experience that mirrors professional environments. This instructional design is particularly valuable for students at the introductory level, who may have limited exposure to firewall technologies. Providing access to authentic, interactive learning experiences helps bridge the gap between conceptual knowledge and applied skills—skills that are essential in nearly every organization with networked systems. Looking ahead, there is strong potential to further enrich the curriculum by revisiting the Foundations in Cybersecurity course. Enhancements could include expanded coverage of command-line interface tools and additional lab-based exercises that reinforce technical competencies. Such adjustments would not only deepen student engagement but also better prepare them for the evolving demands of cybersecurity roles in the workforce.

## 8. LIMITATIONS

Many firewall vendors exist, and even open-source firewalls could have been used in this pedagogy exercise and approach. Without the existence of a classroom full of physical firewalls, future exercises can be undertaken to evaluate other vendors or open-source firewalls that could be used to introduce students to these perimeter security devices and solutions. In addition, there is a limitation related to evaluating whether any cloud-based solutions exist that would eliminate the need to mount a virtual machine image on individual laptops. A limitation related to the theoretical framework or theory to follow as part of this activity is presented. Alternative theories that can be considered relevant to this pedagogy activity are available and could have been approached as part of this study paper. Finally, all students were polled at the end of the course to determine their feedback on using the virtual firewall solution. A limitation arose from not having a pre-course set of questions that asked students if they needed a more significant background in using a command-line interface prior to engaging with the virtual firewalls. The academic literature rapid scan in Table 1 could have also included the word "education" in addition to pedagogy, to possibly result in more found references.

## 9. ACKNOWLEDGEMENTS

Successful technical projects—especially those involving multiple components and collaborators—depend on the dedication of individuals who recognize the value of the work and contribute meaningfully to its success. We extend our sincere appreciation to Richard (Rik) Maerz, Cass Hill, and Troy Gallo of Fortinet for their generous support and collaboration in making open educational resources accessible to students. Their commitment to advancing cybersecurity education through practical tools and industry partnerships was instrumental in the implementation of this project. We also gratefully acknowledge Christopher Eng, a Kean University student and part-time staff member in the Office of Computer and Information Services, for his meticulous efforts in testing the virtual machine and firewall image. His work ensured compatibility with laboratory laptops and helped create a seamless experience for students engaging with the virtual firewall environment.
Finally, we would like to recognize the forward-thinking contributions of Michael Fagioli and Jessica Jones from the Kean Global and Online team. Their innovative vision helped shape the next iteration of the *Firewalls and Secure Computing Enterprise* course, which will feature enhanced instructional elements—including the integration of cybersecurity-themed Escape Rooms—to further engage students through immersive, experiential learning.

## 10. REFERENCES

Dutt, V., Ahn, Y.-S., & Gonzalez, C. (2013). Cyber situation awareness: Modeling detection of cyber-attacks with instance-based learning theory. *Human Factors*, *55*(3), 605-618. https://doi.org/10.1177/0018720812464045

Fortinet. (2024). *Fast Track Workshops Experience the Fortinet Security Fabric in Action.* Retrieved August 14, 2024 from https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/02_Collateral/Brochures/brochure-ftnt-fast-track.pdf

Gampell, A. V., Gaillard, J. C., Parsons, M., Le De, L., & Hinchliffe, G. (2024). Participatory Minecraft mapping: Fostering student's participation in disaster awareness, 48. https://doi.org/10.1016/j.entcom.2023.100605

Gonzalez, C., Lerch, J. F., & Lebiere, C. (2003). Instance-based learning in dynamic decision making. *Cognitive Science, 27*(4), 591-635. https://doi.org/10.1207/s15516709cog2704_2

Haghighi, M. S., Farivar, F., & Jolfaei, A. (2024). A machine-learning-based approach to build zero-false-positive IPSs for industrial IoT and CPS with a case study on power grid security, *IEEE Transactions on Industry Applications, 60*(1), 920-928. https://doi.org/10.1109/TIA.2020.3011397

Hassan, I. (2020). Teaching cybersecurity to computer science students utilizing terminal sessions recording software as a pedagogical tool. IEEE Frontiers in Education Conference (FIE), Uppsala, Sweden, 2020, pp. 1-8. https://doi.org/10.1109/FIE44824.2020.9274268

Oracle VirtualBox. (2024). VirtualBox End-user documentation. Retrieved August 22, 2024, from https://www.virtualbox.org/wiki/End-user_documentation

Rozinaj, G., Vančo, M., Vargic, R., Minárik, I., & Polakovič, A. (2018). Augmented/virtual reality as a tool of self-directed learning. *25th International Conference on Systems, Signals and Image Processing (IWSSIP)*, Maribor, Slovenia, 2018, 1-5. https://doi.org/10.1109/IWSSIP.2018.8439309

Sanchez, J., Mallorqui, S., Briones, A., Zaballos, A., & Corral, G. (2020). An integral pedagogical strategy for teaching and learning IoT cybersecurity. *Sensors, 20*(14), 1-35. https://doi.org/10.3390/s20143970

Veksler, V. D., Buchler, N., Hoffman, B. E., Cassenti, D. N., Sample, C., & Sugrim, S. (2018). Simulations in cyber-security: A review of cognitive modeling of network attackers, defenders, and users. *Frontiers in Psychology, 9*(691). https://doi.org/10.3389/fpsyg.2018.00691

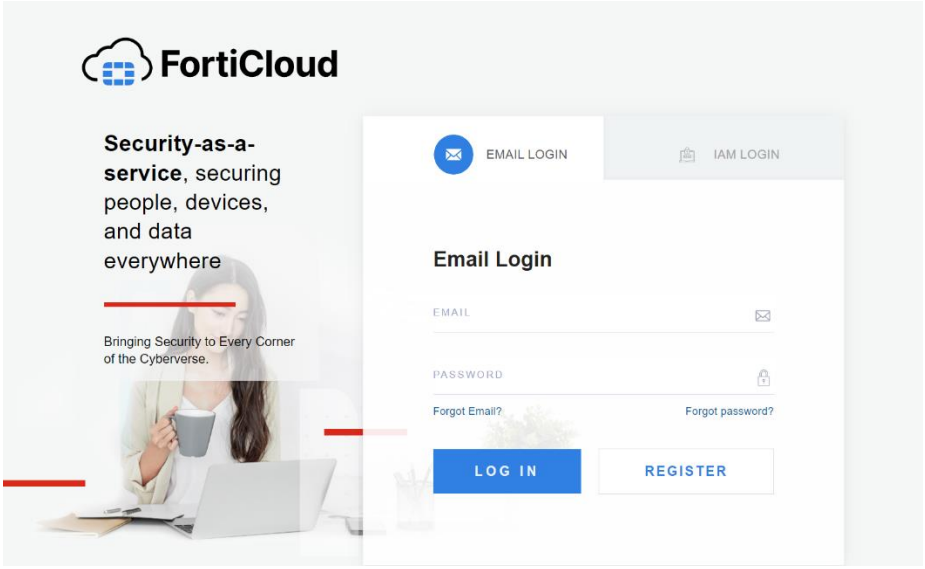
## APPENDIX A

### Fortinet Virtual Firewall Setup and Installation Steps

The steps below include the tasks that prepared the laboratory laptops to run the Oracle VirtualBox and virtual Fortinet firewall solution.

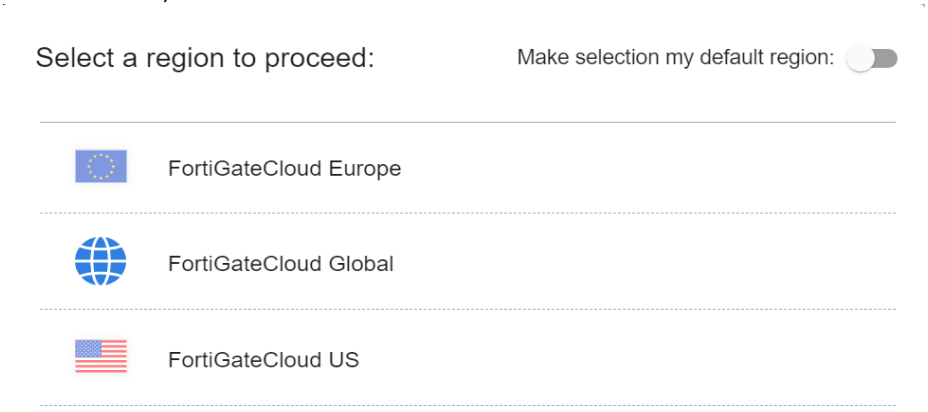
### Download the Virtual Firewall Image

1. Navigate to the https://www.forticloud.com website.
2. From the FortiCloud website, click on the link to register and create a free account.



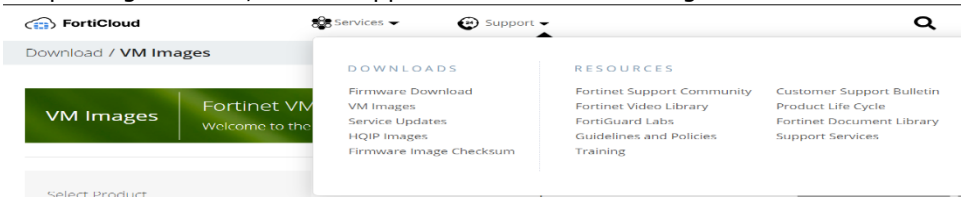

a.

3. After successfully logging into the FortiCloud website, select the appropriate region for your location. In our case, select FortiGateCloud US.




a.

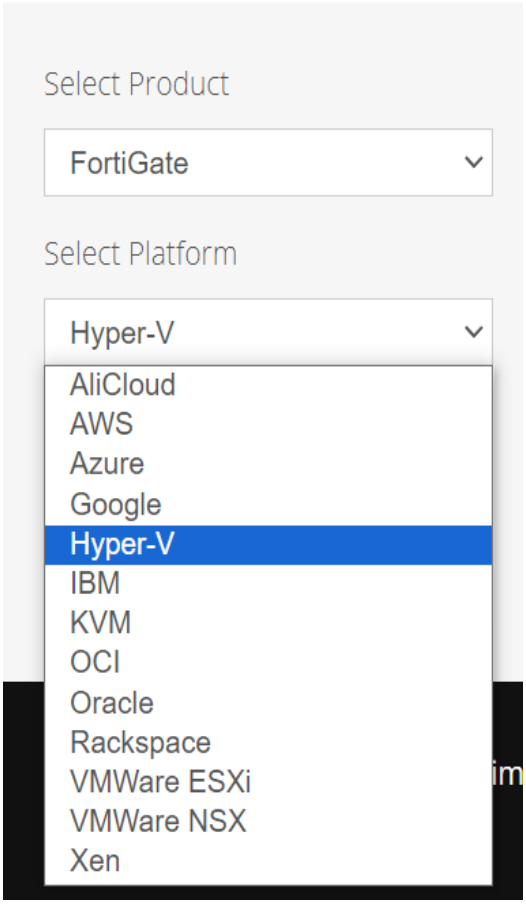
4. From the top navigation bar, select Support-Downloads-VM Images.




a.

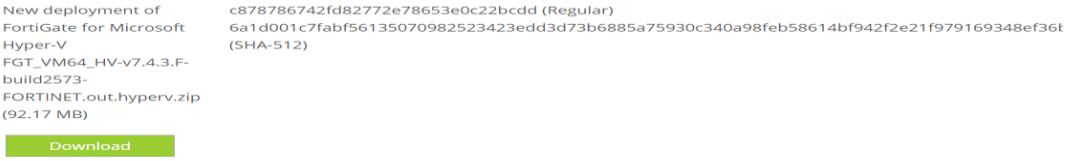
5. From the dropdown menu provided, select the product FortiGate and the Hyper-V platform.

a.




6. Select the FortiGate for Microsoft deployment.

a.




7. Click Download, and make note of the location where the FortiGate virtual firewall image was saved on the laptop hard drive.

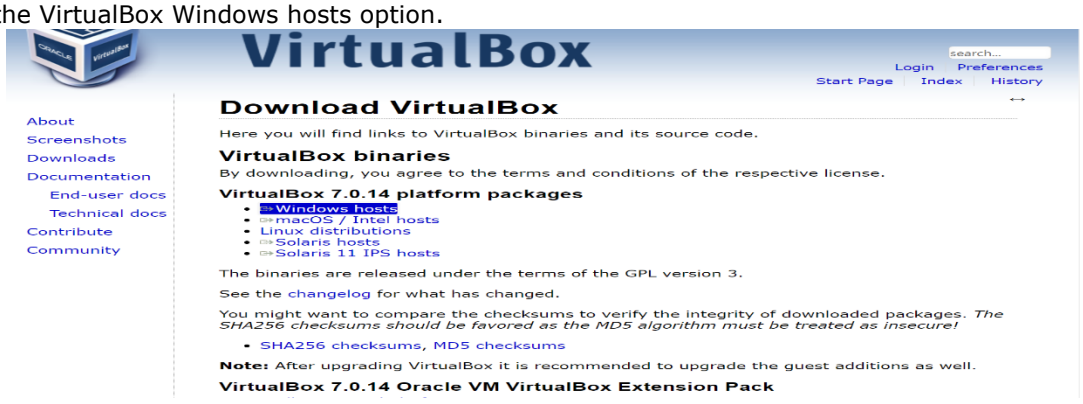
**Installation and Configuration of VirtualBox**

1. Navigate to the website https://virtualbox.org.

a.

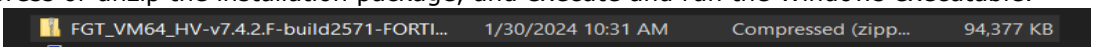

2. From the left navigation bar, click Downloads.
3. Select the VirtualBox Windows hosts option.

a.



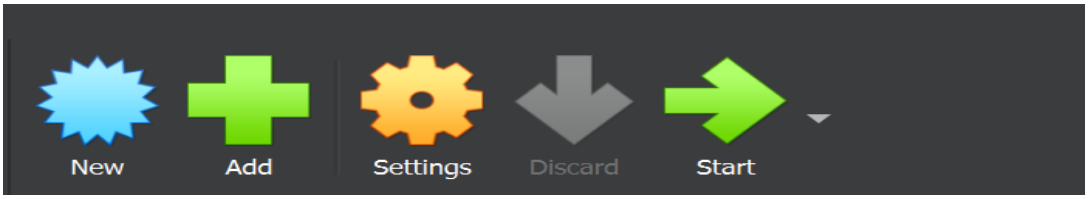

4. Uncompress or unzip the installation package, and execute and run the Windows executable.

a.



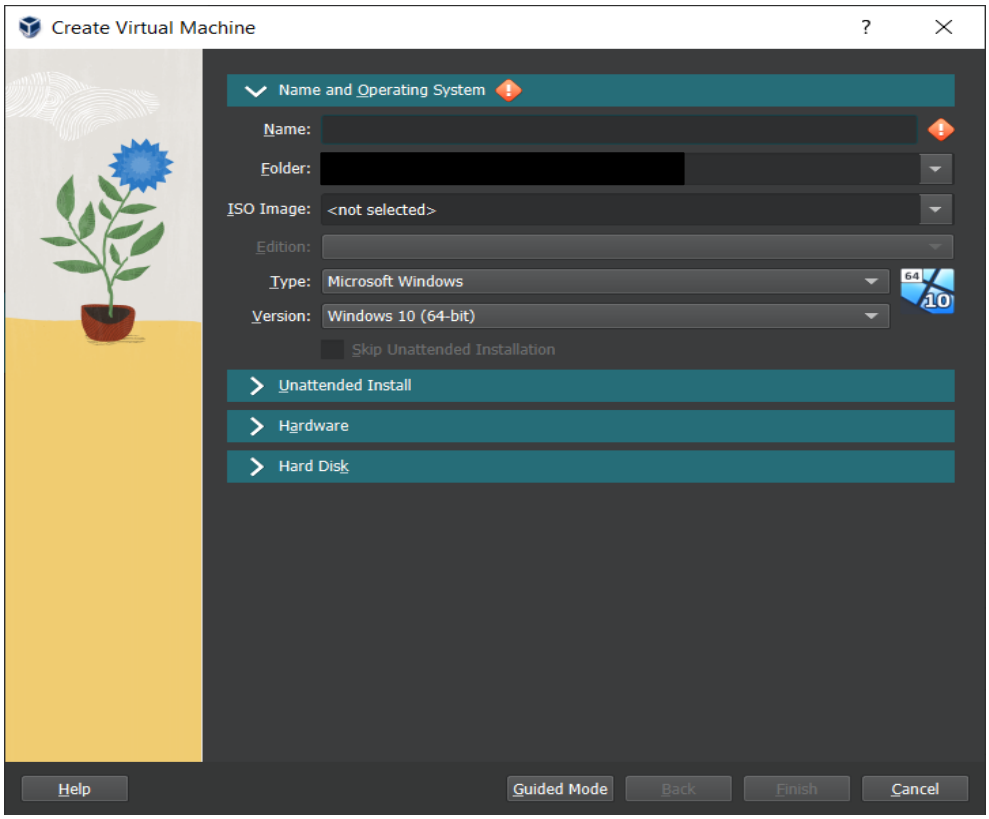

5. From the menu options available, click New to create a new virtual image for the Fortinet virtual firewall.

a.



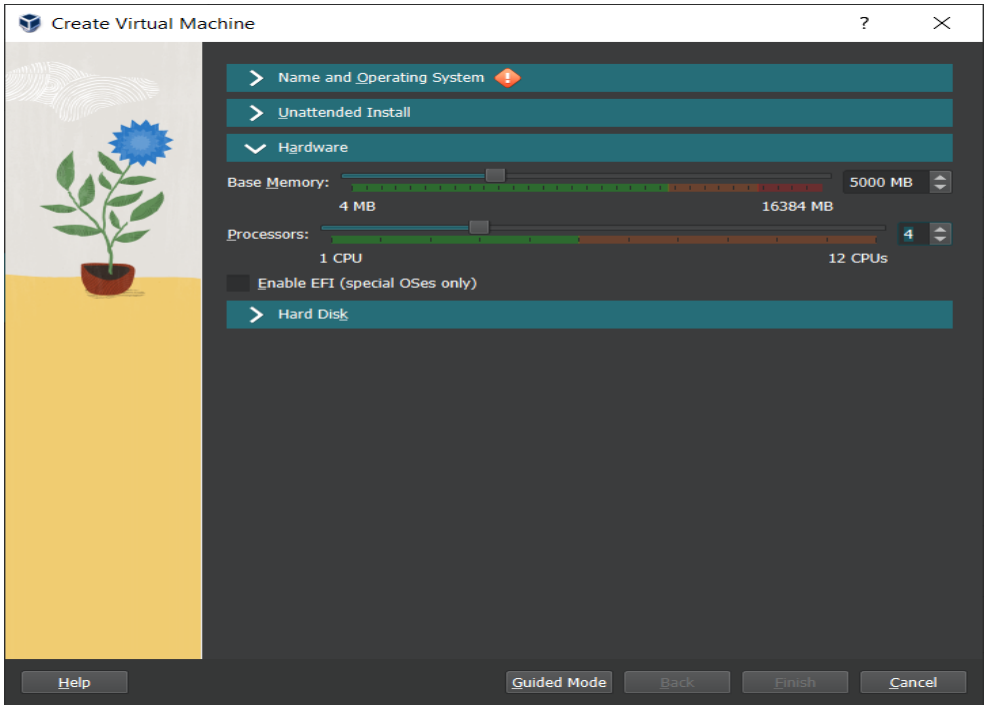

6. Name the virtual machine Fortinet Virtual Firewall

a.

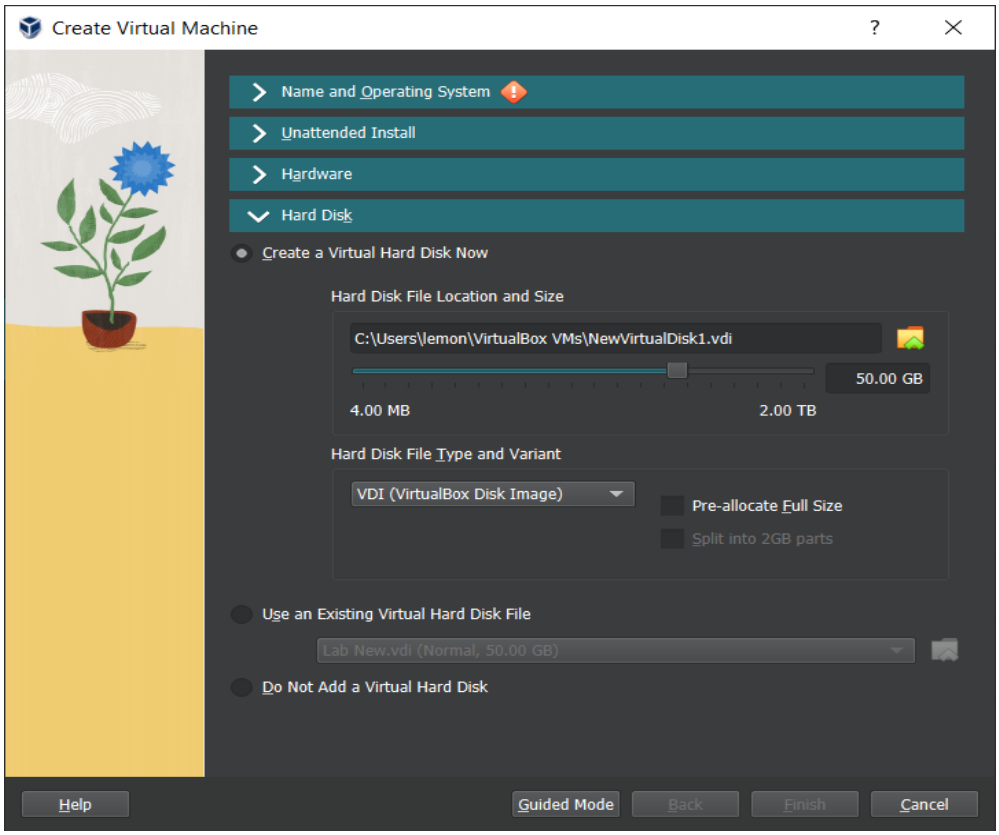



7. Proceed and step through the configuration steps, selecting the Base Memory of 5GB and 4 CPUs.

a.




8. Select the location to store the Virtual Hard Disk and allocate it with 50GB.

a. 


9. When presented with the File Explorer, click on the Virtual Hard Disks and select the downloaded FortiGate VHD image in Step 7 above.

## APPENDIX A

### Starting Virtual Machine – Fortinet Virtual Firewall – FortiOS

The steps and procedures below are utilized to configure the virtual Fortinet firewall on the Cyber Crime Lab laptops. The procedures are essential to ensure future lab experiments and demonstrations can be activated and work properly.

**Command Line Interface**

1. Boot the laptop.
2. Connect to the college Wi-Fi network in the cybercrime lab.
3. Ensure VirtualBox is configured with the Bridged Adapter setting enabled.
4. Login Using Command Line Interface (will be asked to change password).
    a. U: Admin
    b. P: password
5. Ping a site (to ensure connectivity routing outside the lab).
    a. Exec ping www.yahoo.com
    b. Verify connectivity
6. Obtain the IP address of the virtual firewall (use the command line).
    a. Diag IP Addr List
    b. Note Port1
    c. Obtain the IP Address for Port1

**Web Interface**

1. Open a web browser from the said laptop outside of the VirtualBox application.
2. Navigate to the IP address from Step 6 above.
3. Login – same credentials as Command Line Interface.
4. License
    a. Login to https://support.fortinet.com
    b. Set up account
    c. You must check your email – use @kean.edu email.
5. From the web interface – log in to apply the demo license.

## APPENDIX B

### Connecting to and Navigating the Virtual FortiGate GUI

In this exercise, you will have the opportunity to connect to the FortiGate GUI and explore the pre-configured Management interface.

Port1 on FGT-EDGE has been pre-configured to include the following settings, which are not part of the default FortiGate configuration:

• **IP/Netmask**: 192.168.0.101/255.255.255.0

• **Administrative Access**: HTTPS, HTTP, PING, FMG-Access, SSH, and Security Fabric Connection
A password was also set for the default **admin** account.

**Tasks**
1. Return to the **Lab Activity Tab**. Click **FGT-EDGE** in the sidebar menu under **Core**, and then click **HTTPS** to access the **FGT-EDGE** device.
2. Login using the default admin account by entering the following credentials:
**Username**: admin
**Password**: Fortinet1!
3. You have access to the FortiGate GUI.
4. Click **Network** > **Interfaces** and select **Management Network (port1)**. Click **Edit**. You can also double-click the interface. **Note:** Do not change any of the settings currently configured for port 1.
5. The pre-configured settings appear under **Address** and **Administrative Access**.
6. Click **Cancel** to exit without changing any settings.

**Stop and Think**
Security best practices recommend configuring management interfaces with the minimal level of administrative access required. The level of access is usually based on the role of the interface, accessibility to the interface, and the level of authority for users with access to that interface. Consider an organization that has the following infrastructure deployed:
• FortiGate management using FortiManager Cloud services
• FortiGate two-factor authentication via FortiToken Mobile
• Remote APs participating in the organization's Security Fabric

**Set the System Time Background**
In this exercise, you configure the system time on FGT-EDGE to AcmeCorp's local time zone, Eastern Standard Time.
**Note:** For the purpose of this lab, you must select Eastern Standard Time. Making changes to the time zone could disrupt the lab functionality.

**Tasks**
1. Click **System** > **Settings**.
2. Under **System Time**, select **(GMT-5:00) Eastern Time (US & Canada)**.
3. Set **Set Time** to **NTP**.
4. Set the **Select server** to **FortiGuard**.
5. Select **Apply**.

**Create Firewall Addresses and an Address Group**
Firewall addresses define sources and destinations of network traffic and are used when creating firewall policies. Address groups are used to group firewall addresses that require the same firewall policy.

In this exercise, you create three firewall addresses, one for each network. You also create a firewall group that contains the addresses for the Sales and Finance networks. By creating an address group that contains the addresses for both Sales and Finance, you can now configure FGT-EDGE to treat traffic from both of these networks in the same way.

**Tasks**
1. Click **Policy & Objects** > **Addresses** and then use the **Create New** drop-down menu to select **Address** and create an address for the Sales network.
2. Configure the following settings:
• **Name**: Sales
• **Type**: **Subnet**
• **IP/Netmask**: 172.16.10.0/24
• **Interface**: **any**
3. Click **OK**.
4. Click **Create New** > **Address** to create an address for the Finance network.
5. Configure the following settings:
• **Name**: Finance
• **Type**: **Subnet**
• **IP/Netmask**: 172.16.20.0/24
• **Interface**: **any**
6. Click **OK**.
7. Click **Create New** > **Address** to create an address for the DC network.
8. Configure the following settings:
• **Name**: DC
• **Type**: **Subnet**
• **IP/Netmask**: 172.16.100.0/24
• **Interface**: **any**
9. Click **OK**.
10. Use the **Create New** drop-down menu to click **Address Group**.
11. Configure the following settings:
• **Group name**: Sales and Finance
• **Type**: **Group**
• **Members**: **Finance** and **Sales**
12. Click **OK**.

**Apply Antivirus Scanning and SSL Inspection Background**
In this exercise, you create an antivirus profile for Sales and Finance to protect network traffic from virus outbreaks. You also apply full SSL inspection to allow FGT-EDGE to inspect encrypted traffic. When you apply full SSL inspection to traffic, network users may receive a security certificate warning in their internet browser. In this exercise, Bob's computer has been pre-configured to prevent any warnings from appearing.

**Tasks**
1. Return to the **FGT-EDGE** tab.
2. Click **Security Profiles** > **AntiVirus** and click **Create New**.
3. Set the **Name** to Sales and Finance.
4. Under **Inspected Protocols**, turn on all protocol options.
5. Turn on the **AntiVirus scan** and set it to **Block**.
6. Leave the **Feature set** as **Flow-based**. Flow-based inspection takes a snapshot of content packets and uses pattern matching to identify security threats in the content. Proxy-based inspection reconstructs content that passes through the FortiGate and inspects the content for security threats.
7. Under **APT Protection Options**, turn on **Treat Windows Executables in Email Attachments as Viruses** and leave **Include Mobile Malware Protection** turned on.
8. Under **Virus Outbreak Prevention**, turn on **Use FortiGate Outbreak Prevention Database** and set it to **Block**. This allows the FortiGate antivirus database to use third-party malware hash signatures curated by the FortiGuard to block detected viruses before a FortiGuard signature is available.
9. Click **OK**.
10. Click **Policy & Object** > **Firewall Policy**, click **Sales and Finance**, and click **Edit**.
11. Under **Security Profiles**, turn on **AntiVirus**. Use the drop-down menu to select the **Sales and Finance** profile.
12. Use the **SSL Inspection** drop-down menu to select **deep-inspection**. This turns on full SSL inspection so FGT-EDGE can inspect encrypted traffic.
13. Click **OK**.

14. Connect to the **Bob** device.
15. Run Chrome and click the browser bookmark **EICAR**. This website contains a file that you can use to test your antivirus scanning.
16. Under the **Download area, use the secure SSL-enabled protocol https, and** click **eicar.com**.
17. FGT-EDGE blocks the file from downloading.

**Add a Default Route Background**
In this exercise, you add a default route to the FortiGate that the FortiGate uses to send traffic outside of the internal network.

**Tasks**
1. Click **Network** > **Static Routes** and click **Create New**.
2. Set **Destination** to **Subnet** and leave the destination IP address set to 0.0.0.0/0.0.0.0.
3. Set **Gateway Address** to 100.65.0.254.
4. Set **Interface** to **ISP1 (port6)**, the internet-facing interface.
5. Click **OK**.
6. To test internet connectivity, click **>_** in the top right-hand corner to connect to the CLI console.
7. Type the command execute ping 8.8.8.8 and press Enter.
8. The FortiGate connects to the internet, producing an output similar to the screenshot below:
9. Close the CLI console by clicking on the **X** in the upper right corner.

**Note:** Fortinet provided the subset of laboratory examples provided in Appendix B for use by the faculty and students (Fortinet, 2024, August 14).