CYBER DEFENSE PLANNING IN TABLETOP EXERCISES AND CONSIDERATION OF A FRACTURED FLAW THEORY FOR SECURITY APPLICATIONS

by

Patrick Kyle Kilroy II

Liberty University

A Dissertation Presented in Partial Fulfillment

Of the Requirements for the Degree

Doctor of Philosophy

Liberty University

2024

CYBER DEFENSE PLANNING IN TABLETOP EXERCISES AND CONSIDERATION OF A FRACTURED FLAW THEORY FOR SECURITY APPLICATIONS

by Patrick Kyle Kilroy II

A Dissertation Presented in Partial Fulfillment

Of the Requirements for the Degree

Doctor of Philosophy

Liberty University, Lynchburg, VA

2023

APPROVED BY:

_____

Dr. John Bentley, Committee Chair

_____

Dr. Steven Ufford, Committee Reader

_____

Dr. Fred Newell, Department Chair

ABSTRACT

Cybersecurity threats endanger every part of American life. Security and emergency preparedness professionals plan and prevent cyber-attacks using tabletop exercises. The tabletop exercises establish the risks and protection strategies for multiagency threats, thus, various agencies and industrial partners must work together in these training events. The purpose of this grounded study will be to develop criteria for selecting tabletop participants and explore the risks of participation. An additional consideration is the impact of the sponsoring agencies' agenda on the value of the outcome for the participants. There is sufficient evidence to justify the investigation of these issues. Failing to include the correct participants has led to significant data breaches in the last few years. Participants may also place themselves in more significant harm through participation. The publication of the outcomes of tabletop exercises, including security gaps, causes grave concerns. The primary theory guiding security concepts is Walodi Weibull's 'weakest link theory;' however, the flawed fracture theory may be invaluable as an alternative to the weakest link theory. The study design will qualitatively evaluate recent critical infrastructure exercises. Historical literature reviews and current qualitative efforts (ongoing exercises, action items, interviews, and surveys) provide the basis for improvement. A survey with 39 participants, four in-depth interviews across multiple business sizes, and one federal employee yielded findings related to noncompliance, tabletop baggage, and cascading events.

Not having the correct participants leads to weaknesses across tabletop events. Having a missing organization or participant causes complications in response and leads to unrealistic responses. The current consequence of participating in a tabletop exercise was that although participation improved responsiveness and security, smaller partners may face a disproportionate increase in risk. Finally, the agenda, goals, and objectives are all impacted by the tabletop exercise's

sponsor. The prevalence of organizational noncompliance was unexpected. Theoretically, expanding from the weakest link model to the fractured flaw model will significantly improve how security professionals manage risk and survivability. Improving tabletop exercises will enhance the nation's emergency preparedness and potential resiliency.

Keywords: critical infrastructure, cyber security, cascading events, CIKR, tabletop exercises, weakest link, fractured flaw

Acknowledgments

This researcher completed this effort under the gracious, encouraging spirits of Dr. Bentley and Dr. Ufford. Dr Bentley and Dr. Ufford are uncommon men whose remarkable and unwavering spirits provided guidance, inspiration, and hope. I count myself among those fortunate enough to cross their paths. From our first meeting, I jealously guarded every moment and hung on to every word of advice, even if difficult for me to implement. Their extraordinary commitment to making the world a better place serves as an inspiration. Thank you to my wife, children, and friends who encouraged my countless nights chasing this research to improve cyber security. Thank you to my professor's whose constant reminder to keep everything in a Biblical context helped me through of the scariest moments of my adult life. Thank you to Gretchen Lapp whose wisdom and final notes made all the difference. Thank you to the Lord my Savior for an opportunity to know a life lived with purpose.

Table of Contents

List of Figures

List of Abbreviations

Critical Infrastructure and Key Resources (CIKR)

Chemical, Biological, Radiological, Nuclear, and high yield Explosives (CBRNE)

Foreign Intelligence Service (FIS)

Informational Technology (I.T.)

National Incidence Management System (NIMS)

Operational Technology (O.T.)

Tabletop Exercises (TTX)

Supervisory Control and Data Acquisition System (SCADA)

Protective Measure Index/Vulnerability Index (PMI/VI)

System of Systems (SoS)

CHAPTER ONE: INTRODUCTION

Overview

The world has changed faster in the last 50 years than at any other time in history. The rise of technological innovations and new things has grown exponentially (Jorgensen, 1999). Crime, terror, and war have kept pace with the ever-changing world and have leveraged technology into new means and methods (Davis, 2000). Despite the latest venues to commit crimes, even modern crimes in the digital space retain historical analogs. Cybercrimes have brought a modern threat to humanity, businesses, governments, and more. Cybercrimes, cyber warfare, and cyberattacks extend into every aspect of digitized American life and represent a unique converged threat to organization security (Aleem, 2013). Technological advances have not only happened on the positive side of humanity but also on the cybercriminal front. As the world grapples with responding to cyberattacks, identifying the areas most vulnerable to attack is crucial to their protection. Tabletop exercises often help identify gaps and weaker segments.

The Department of Homeland Security has divided critical infrastructure into 16 sectors. The critical infrastructure sectors are nuclear, financial services, food and agriculture, chemical, energy, dams, emergency services, government facilities, information technology, commercial facilities, wastewater, defense industrial base, healthcare, critical manufacturing, and communication. Recognizing these separate sectors highlights the interdependency of multiple infrastructure areas. A common way of planning for emergencies is tabletop exercises. They allow for the role-playing of an emergency and are a common form of emergency management preparedness. Tabletop exercises allow for the interconnection of various sectors, departments, and agencies to bring their unique perspectives. The results then inform additional training, defense development, and planning tools. Most realistic tabletop exercises often require multiple

sectors to share information, resources, and participants to benefit from the training. All functional sectors need practical scenarios that foster communication and cooperation.

Emergency and incident response has also highlighted the interconnected world. Emergency communication systems connect to municipal networks. Emergency calls often depend on a city's internet networks and computer systems that handle other more mundane operations, from taxes to park schedules (Kitchin, 2020). The city's network also depends on local power generators, personnel showing up to work, fuel for vehicles, functioning radios, and open radio frequencies, all of which add to critical infrastructure (Moteff, 2004). Organizational security depends on each system working cooperatively; the more significant the system, the more elements must work together.

The Department of Homeland Security and the Federal Bureau of Investigation identified a protection gap in the industrial and critical infrastructure in the mid-1990s (Moteff, 2004). The commercial portion of the infrastructure represents portions of the economy important to national security but not controlled by the federal government. The critical commercial infrastructure can include hospitals, banking, power distribution, the chemical industry, etc. The government, private, and industry formed partnerships to improve security in an ever-changing world. The idea was to share best practices to secure public and private sectors and allow private partners to identify emerging threats.

Critical infrastructure protection requires commercial and industrial partners and the federal government to cooperate in defense (Berkely, 2010). Critical Infrastructure is owned and operated by both the government and industrial partners. Despite its high-security value, much of the infrastructure that allows the United States to function depends on commercial or private owners. Private entities own significant portions of infrastructure in the United States. The

internet, water treatment, waste disposal, fuel distribution, and more are all handled and owned by private industries. Private enterprises own approximately 85% of critical infrastructure (Pfeifer, 2018). Because of the shared reliance on this infrastructure, private sectors and governments must cooperate in the shared protection. These divided parties and interests represent a struggle to link together for emergency planning and security. A tabletop exercise is the most common way to protect the entire system. Tabletop exercises provide an opportunity for each stakeholder to a more extensive network to share information and discuss their role in the overall security of the group.

Planning and preparing for a tabletop exercise includes many aspects, including the scenario, location, participants, data collection, and performance measures (Mitchell, 2019). Although each element of an exercise is important, little research exists on selecting participants for domestic cyber warfare scenarios (Mitchell, 2021). Selecting participants from each sector is essential; ensuring stakeholder participation is often vital in defining and obtaining the buy-in of needed changes following an exercise (Agner, 2021; Mitchell, 2019). The historical approach has been that all participants benefit from being involved. Recent studies show that more than 84% of participants consistently completed exercises to gain significant knowledge or identify needed changes to operational procedures (Mitchell, 2019). A secondary risk is failing to identify gaps in a scenario through missed issues. Not including all participants could cause missing problems. This document characterizes current research through a formal literature review. A potential framework of attack vectors may provide insight into critical, nice-to-have, and extra participants. Outside of procedures, tabletop exercises provide the backbone for cyber-emergency-preparedness and represent the only proper way to drill on cyberattacks.

Background

For years, tabletop exercises trained emergency responders. Tabletop exercises became a standard method for dealing with emergency response issues, and the National Incidence Management System (NIMS) training mandated their use. Tabletop exercises allow the team members to participate in realistic activities with multiple agencies or functions within an agency to prepare for future emergencies (Department of Homeland Security, 2003).

Historical Background

Tabletop exercises allow for role-playing activities within a single agency or across multiple. The scenario allows the rehearsal of roles and discussion of responses to a given event. Personnel roles and responsibilities validate the content of a plan through discussion of their roles and their responses to emergencies, execution of responses in a simulated operational environment, or other means of validating responses that do not involve using the actual working environment. Exercises are scenario-driven with an initiating event and often have follow-on events that mirror real-life event follow-on effects. Follow-on events include additional attacks, weakened systems failure, or temporary resource depletion. For years, tabletop exercises trained emergency responders for events, large crowds, complex interagency interactions like the Olympics, high-hazard or complex operations, and even complicated medical procedures (Johnson, 2019). Tabletop exercises helped to prepare for hurricanes, floods, and wildfires. Participants have been as varied as law enforcement, EMTs, medical doctors, daycare workers, bankers, trash truck drivers, and water treatment operators.

Historically, single agencies conducted emergency preparedness exercises. Until the early 2000s, interagency cooperation consisted of memorandums of understanding and mutual aid agreements in which limited capabilities mandated cooperation. Firefighting capabilities were

the most commonly shared resources. Following September 11, 2001, Commission's Report, the world set out on a new era of cooperation. The war on terror was waged at home as much as overseas. The cooperation efforts saw information sharing. Fusion centers were developed to handle the sharing of multiagency information. Some fusion centers went on to become industry specific.

During this post-9/11 reconfiguration, cybersecurity moved away from single-agency protection perspectives and began considering that there were many more cybersecurity-related elements than maintaining anti-virus software. From 2001-2020, several other dramatic changes were underway. Cyber vulnerabilities moved from computer-only to all old and new operation technology. The internet and computers moved from being the primary threat to only a tiny piece of the overall picture. The threat of attacking a computer was the ability to steal data, banking information, or lock someone out. Controlling the building meant shutting down an entire company, locking the doors, catching printers on fire, or even using a facility's safety design to cause it to self-destruct. By 2020, the problems had moved to protect the internet, computers, instruments, and operational systems. Unfortunately, this transition quickly led to the realization that systems subversion happens throughout the supply chain. The future will include protecting every step of the supply chain. Government agencies validated supply chain problems through sabotage detection in control valves inside government facilities' control systems and even additional router switches and network equipment. Foreign Intelligence Services (FIS) planted routers and switched gear in original procurements.

The underlying theory providing context for these issues is the weakest link theory (Arce, 2003; Hirshleifer, 1983). The weakest link theory proposes that the attack or breach often occurs on the weakest or least protected member of a group. Regardless of the motivation of the threat

actors, typically ideological or financial, emergency and security professionals returned to standard mitigation methodologies. Tabletop exercises emerged as the preferred method to ensure all 'links' were covered. Tabletop exercises measure success through post-meeting actions, procedure changes, lessons learned, and recognition of risks (Holloway, 2007). From the beginning, the research has focused on getting scenarios correct and providing effective methods of capturing participant and agency inputs. Recent events developed complicated true-to-life multiple elements scenarios, but recreating the interconnected network remains challenging. No way currently exists to provide insight into the security chain elements outside of participation, and all efforts to understand a non-participant are conjectures or projections. Participants are lured into believing they are improving their security but may walk away with a false sense of security. Participating in the scenarios may flag smaller agencies as targets and identify their connections to more critical targets. The current efforts are indeterminate in aiding those participating and may not be closing the gaps for non-sponsoring agencies.

Social Background

Socially, cybercrimes and critical infrastructure specialists represent the two spectrums of aggressors and protectors, with a whole of victims and citizens in the middle. The essential variables include the markets, sectors, and individuals that comprise the security framework. Social concepts around emergency preparedness include rehearsed drills that test participants' capability to respond to an incident. Most of society engages in emergency drills, whether fire, earthquake, or even active shooter drills in schools, or much more complicated like those practiced by the armed forces. Fundamental to each is a sound understanding of the hazard, careful evaluation of the response, and the lessons learned from the drill incorporated into work processes.

In the cybersecurity world, drills through tabletop exercises are a new phenomenon. In an interconnected world, shared networks, software, and access require inter-personnel engagement. The historical protection methodologies included denial and prevention of attacks. The more sophisticated modern prevention methods include threat hunting, active deception, and honey traps. As it sounds, threat hunting involves targeting the attackers and eliminating the threat. Deception relies on camouflage and making the targets appear less attractive. Honey traps are typically enticing targets with no value but often include malware or viruses disguised as valuable information. Participants have deployed entirely fake network segments on the cutting edge of cyber protection, mirroring Patton's ghost army or World War 2, changing airplane transponder information, or re-numbering Navy Seal units (Beyer, 2015). The active deception provides opportunities to sabotage attackers and installs intrusion detection software and hardware. Protection specialists use the active act to provide offensive counterintelligence efforts through tracking and misinformation. These efforts are the most effective when they protect the potential risk surface. Anyone not included instantly creates a pre-existing gap or weak link in the chain.

Theoretical Background

The weakest link is the most common theory underpinning the protection of critical resources in most U.S. training programs (ASIS, 2010). The weakest link theory underpins training, safety, and all security efforts in which multiple components or systems are together (ASIS, 2010). The weakest link theory conceptually is a chain in which tension is placed on the ends until the lowest point breaks or opens up. This theory targets the most vulnerable points for fortification. In the weakest link, vulnerabilities shift from one area to the next as weaker areas are protected.

When multiple events occur, the probability of overall failure is multiplicative. Numerous incidents materialize in real life as attacks during natural disasters or multifaceted attacks from terror or organized crime/state actors. Cybercriminals typically attack more than one front. Cyber-attacks serve as the first line of attack for many physical attacks. The 2022 Russian invasion of Ukraine demonstrates the weakening of a target via cyber efforts before armed forces entered the country. Cyber-attacks cause disruption and chaos. Cybercriminals attacked Louisiana during a hurricane during the first documented successful large-scale ransomware attack.

The combination of hazards or events can lead to failures of systems in a water-fall or cascading type scenario. Today, the risk of cascading events represents a continuity of government risk. Globalization's interconnectivity and technological combination make events hard to overcome and predict (Helbing, 2013). Cascading events represent the next series of challenges in tabletop exercises. Cascading events are like toppling dominoes; a small initiation can have a much more significant impact. The critical factor is that a small initiating event causes a chain of events with an exponentially more substantial impact (Khan & Abbasi, 2000; Reniers, 2009). The triggers for cascading events can be as simple as a severe weather event. The 2021 extreme weather event highlighted the interconnectivity between the electrical grid and the water distribution (Busby, 2021). Cascading events with multiple attacks and multiple attack vectors represent the most realistic threats and the penultimate value of tabletop training events.

The freezing temperatures took out power generation across Texas in February 2021 (Nazir, 2021). The lack of the ability to distribute water allowed pipes to freeze, and many Texas homes were left without power for more than 24 hours during subfreezing temperatures (Nazir, 2021). Although this was a weather-related emergency, the event demonstrates the effect a

cascading event can have. Citizens without power quickly ran out of water. As the temperature dropped, the pipes froze, and the entire distribution became damaged. Even after power restoration, the infrastructure damage took months to repair (Busby, 2021). Eventually, 111 people perished, with an estimated $40-50 billion in financial impacts (Whelan, 2021). These recent cascading events have furthered the recognition that infrastructure is interconnected and hazards in even commercial facilities can impact government capabilities. A challenge to the current theory is that it fails to explain cascading events. Once the chain breaks, this model does not describe the follow-on effects or events coming from additional attacks.

Situation to Self

The motivation for researching this effort is multifaceted. An immediate, repetitive need is the identification of participants in drills and exercises. Who affects who and how the potential impact flows from one area into another is a critical dynamic in the current threat climate. The complicated System of Systems (SoS) approach represents the network from one infrastructure sector to another. The next level, in detail, finds that within a single industry, these systems consist of even more complicated independent businesses that relate to each other. A constructivist paradigm will guide the study through idea exploration, proposition, explanation or evaluation, and action. The area of opportunity to make a difference is significant, and all engagement improves overall security. Strategic involvement will allow for the maximum usage of limited emergency preparedness resources.

In a 2020 interview, General Petraeus stated that cyber threats represent the greatest threat to the United States' national security (Mitchell, 2021). Funding is insufficient to deal with threats from every possible vector. The budget in the United States for 2022 included $15.6 billion, with 72% earmarked for the Department of Defense (Stone, 2023). The funding for

cybersecurity does not include the portions of typical operating budgets allocated to cybersecurity. Globally, the current estimate on cyber defense budgets is more than $188 billion (Stone, 2023). Defending critical infrastructure is complex, and emergency practitioners ensure adequate protection. Tabletop exercises in which security evaluations and drills are the primary means for providing sufficient security measures across critical infrastructure. Any missing gaps in tabletop exercise either through lack of participation or competence create critical security gaps which can lead to security vulnerabilities. Outside of the National Institute of Standards and Technology (NIST) checklists and scanning software, the tabletop exercise is the most effective (and standard) tool used in cybersecurity response and protection (Berghel, 2007; Weber, 2018). Recent exercises that left our members or included the wrong participants led to billions of dollars in losses, sensitive data exposure, and even death.

The need for a robust cybersecurity paradigm is critical to the survival of the United States. A gap in cybersecurity can directly undermine every defensive and offensive measure in the arsenal. The risk is factual, every aspect of modern life is at stake, and it may not even be clear that an attack is underway. A failed bank, a run-on stock caused by planted information, and even a stock market crash triggered by automated software are all within the current cyber criminal's capabilities. More significant threats extend from detonating nuclear warheads remotely in their silos, inside submarines, to simple and insidious mass poisonings conducted with in situ chemicals in water treatment facilities everywhere in the United States. The only thing in common with the various modalities of an attack is using the tabletop exercise to generate defense responses. Law enforcement will not identify a breach for years or months following an attack. The simple tabletop exercise is the most effective way to safeguard these multi-agency threats.

Problem Statement

Tabletop exercises routinely miss key partners, leading to deep cybersecurity and emergency response preparation gaps. Leaving out a single entity has led to local, state, and federal breaches. Recent tabletop exercises missing a single key partner compromised the Georgia Bureau of Investigation, the South Carolina Law Enforcement Division, and the National Nuclear Security Administration. All three organizations failed to include their local internet service provider. The local provider ended up being the point of attack, and all three had their data sets compromised. Currently, there is no guidance or research on selecting participants. The current approach of including only those interested does little to protect all threat areas. The participants that show up may not even be the correct participants from each organization. The problem is there is no guidance on who to include, the risk of their participation or non-participation, and the impact of the sponsoring organization in tabletop exercises.

Participation in tabletop exercises highlights a bigger problem with the current security theory. The weakest link theory fails to describe or predict security risks. Fracture mechanics is the scientific study of materials and how they break and provides a better predictive perspective of security risks posed by cybersecurity. Fracture mechanics give a plausible and predictive explanation for how overarching issues impact entire systems and how single issues can overcome much more extensive procedures. The weakest link theory assumes every link in a system connects linearly to the next and fundamentally fails to describe the actual behavior of a much more complicated real-world system.

Psychological egoism or selfishness at the organizational level may play a role in creating security gaps. The sponsoring agency drives the tabletop exercise objectives and influences the protection of the group as a whole. The sponsoring agency oversells the drills with a broad

spectrum of good intentions, but the agency's objectives are all that matters at the end of the day. The potential behavior of offering protection to meet agency needs of only the sponsoring agency is a legitimate concern.

Purpose Statement

The purpose of this research is to provide tabletop exercise guidance to participants and participation risk and evaluate the impact of the sponsoring organization's agenda. This qualitative study will show that tabletop exercises routinely miss key partners, leading to compromised security. The world is only one cyberattack away from falling apart, and the most effective tool for combatting these attacks is the tabletop exercise (Mitchell, 2021). This study will enhance our understanding of cybercrimes and cybersecurity by analyzing the effect of missing tabletop participants in cybersecurity response exercises and potential causes. The primary historical theory guiding security (and cybersecurity) is Walodi Weibull's weakest link theory security application, in which the lowest component defines strength or survivability (Aleem, 2013; Zok, 2017).

The researcher has identified that not only do missing participants compromise security, but the underlying theory may not wholly describe observed system behavior. The flawed fracture theory provides a superior alternative to the weakest link theory and may better fit cascading events. The flawed fracture theory represents a novel approach to describing terror events, incorporates entity size in determining strength, deals with overarching external stresses, and explains cascading events. The study design will qualitatively evaluate recent critical infrastructure exercises in which missing participants led to dangerous cyber events. A single missing person led to the "outing of the blue," sinking of a cargo ship, and breaches in the

nuclear weapons program. Outing the blue was the release of law enforcement's personal information, including addresses, and family information onto the dark web.

Significance of the Study

Tabletop exercises conducted in the last ten years have proven the importance of including the correct participants and the disastrous consequences of leaving others out once an event happens. Incomplete tabletop exercises led to the compromise of the FBI databases, overturned ships, and crashlanding of airplanes, but effective practices stopped recent attacks on the United States power grid by Russia. The Georgia Bureau of Investigation (GBI), South Carolina Law Enforcement Division (SLED), and the Department of Energy National Nuclear Security (NNSA) administration agencies all provide examples of top-notch cybersecurity protocols but highlight the vulnerabilities intended mitigated with tabletop exercises. The South Carolina Law Enforcement Division protects the state from cybercrimes. Still, SLED could not preserve its network following an event previously role-played in a tabletop exercise. In 2021, SLED's Internet Service Provider (ISP) breached, allowing access to all protected law enforcement information (SCCIC, 2021). Emergency preparedness managers at SLED left the ISP out of previous tabletop exercises despite discussion that they might be necessary. The personal addresses, emails, and cell numbers were all published in the attacks called "Outing the Blue" (SCCIC, 2021). The long-term consequences of this breach are unknown, but the cause was a failure to include a key participant.

Emergency preparedness managers conducted a tabletop exercise around the port authorities in Charleston and Savannah. For Savannah and Charleston, invitations went to all possible parties, but emergency preparedness managers forgot the vendors who created the software that calculated the loadout of ships in the harbor. The Golden Ray overturned in the

port on September 8, 2019, after being fully loaded with cargo and fuel. The Golden Ray's valuation was $62.5 million, with a cargo value of $142 million. The ship and all cargo were a complete loss, not including the impact of creating a shipping blockage. The Golden Ray accident initially appeared to be a chance mishap and has been determined to be caused by a human error with software. Others believe this could happen again through a malicious cyber attack.

The study's significance will extend directly into the conduct of future training and planning exercises. Identifying missing participants will prevent significant gaps in protecting the United States. The concepts can extend into similar areas, including the planning of emergency preparedness exercises. Tabletop exercises not only test emergency response planning before an event but are also used to prepare future responses.

The study's practical significance will be a guide that will help prepare emergency planning events. Organizations from the Department of Homeland Security, Army Cyber Command, industrial partners; ``local schools could directly benefit from a recommended conceptual framework. Effectively executing the concepts and guidance could influence the entire emergency preparedness community, even if only in a small way (Agner, 2021; Schlanger, 2021). All improvements are significant, even if they only prevent one event.

Research Questions

The research will seek to understand and identify the core characteristics and functional areas of participants in tabletop exercises in contemporary and past events. The goal will be to identify operational and organizational recommendations. Tabletop exercises in cyber incidents are unique in that coordination across government, state, local, and industrial participants is necessary (Mitchell, 2020).

RQ1: What is the impact of having the wrong or missing participants in a tabletop exercise? The primary question from anecdotal information is the impact of leaving potential partners out. No ground rules are the basis of the minimum participants' roles and experience. There is a high likelihood of mismatched skill sets, employee participation in an exercise, and missing partners. Anecdotal data has pointed to issues resulting from the wrong people participating.

RQ2: What is the consequence of participating in a tabletop exercise? Does this cause additional risk? Based on an agency participating, does it increase the overall risk of smaller partners? Obscurity protects many smaller entities. Participation may cause a significant threat to more minor participants. A small daycare or a wastewater operator may not appear to be an attractive target; however, after participating in an exercise, the results are often published as open source. The small business or municipal service provider moves from non-target to a high priority. Some effects even include documentation of known weaknesses and identified security gaps. Participants are concerned that participating may make themselves more vulnerable to future attacks.

RQ3: Do the agenda, goals, and objectives impact the outcome of the tabletop exercise's effectiveness? What impact does the sponsoring agency agenda have on the overall protection outcome? The purpose of protecting self-interests may lead to gaps elsewhere. The participation risk is not explained or captured as a risk to participants, and the common belief that all benefit from participation may not be accurate.

The theoretical research question of understanding the fractured flaw framework versus the weakest link will become apparent as the connection to similar distributed flaws regardless of the originating cause. The researcher will address the theoretical research question based on the

summation of the lower-level data. The materials approach and transition from weakest link to fractured flaw provide a basis for moving to a more sophisticated and accurate theoretical basis for security.

Summary

Cyber threats represent a difficult challenge to national security. The only effective mitigation is tabletop exercises in cross-sector events. There is no guidance on who should make up the tabletop team. Leaving companies, groups, or even one person has disastrous consequences. There are also enormous risks for smaller agencies and business partners to participate. What happens to a small business? Do they walk away safer? Another final concern is that the sponsoring agencies may heavily affect the tabletop exercises to meet their agency needs to the harm of other participants. This study will evaluate Walodi Weibull's weakest link theory and propose a better alternative for assessing security issues through the fractured flaw framework. The study's practical significance will be guidance on emergency planning events and an improved theoretical framework. Effectively executing the concepts and direction could influence the entire emergency preparedness community, even if only in a small way (Agner, 2021; Schlanger, 2021). All improvements are significant, even if they only prevent one event.

CHAPTER TWO: LITERATURE REVIEW

Overview

Cyberattacks represent a clear and present danger to the United States. Although there are many elements to cybersecurity and cyber defense, one of the most challenging elements of cybersecurity is the interconnectivity across multiple organizations. From an advanced perspective, individual organization tabletop exercises are a common way to prepare for responding to cyberattacks. Current research in emergency preparedness exercises or incident command evaluations does not address who should participate in multi-partner issues.

The investigation included scholarly articles on tabletop exercises and cybersecurity and critical infrastructure. Approximately 70% of the research on published tabletop exercises focused on medical emergencies, incident command, and fire response and included the results from individual evaluations. The remaining 30% of the study deals with terrorism and critical infrastructure. The citation percentages values came from 400,000 documents in Google Scholar, access to the Army Cyber Institutes library, the Department of Homeland Security, the FBI's Cybersecurity Infrastructure Security Agency, and the Department of Energy's National Laboratories Office of Science and Technology Bridge. Inside the 30% set, an even smaller subset deals with cybersecurity. A sampling accompanied each successive pull to see the type of material in each document. Sometimes, the tie to cybersecurity is left as a root cause for a single-point failure and does not represent a persistent or active threat.

Of the references evaluated for inclusion, more than 89% come from peer-reviewed research, and 11% come from other sources or may be related to a tabletop exercise. The needed references to Executive Orders, criminal codes, and government sources are peer-reviewed. Three out of 46 were from newspapers or periodicals that would not meet the peer-reviewed

requirements; two were specific information relayed by a government agency that was not peer-reviewed nor qualified as a professional check. A working library captures relevant information for this research and future efforts. The dynamic library consisted of the cyber services of the Amentum Technical Services Operations Support Group Cyber Team and a United States intelligence agency data set.

Theoretical Framework

The theoretical framework of weakest link postulates that security is only as strong as the weakest point. Every organization and individual within a system represents a security risk to that system. Much like a chain pulled until breaking, security means a design of scenarios where the weakest point is the first to fail. This weakest link theory, endorsed by the American Society for Industrial Security (ASIS), serves as the basis for security protection theory.

Weibull's Weakest Link Theory

The weakest link theory has its early roots in the mathematical representation of material strength. Walodi Weibull was a Swedish engineer most widely known for the Weibull distribution, which bears his name. In the late 1930s, he postulated that the strength of a material solid is the summation of the individual element strengths. The Weibull formula in Figure A where $S_o(\sigma)$ is the survival probability of element I at stress σ and N is the number of elements comprising the solid (Zok, 2017), as shown in Figure 1.1.

Figure 1.1

Survivability Equation

$$S = \prod_{i=1}^{N} S_o(\sigma)$$

Specifically, his theory stated that the survival of the whole was limited to the strength of the weakest link (Zok, 2017). Significantly, the Weibull models are the basis for all modern material strength models. The survivability of a component is related to flaws in the substance. Security flaws dictate security strength by expanding the theory to security applications (Aleem, 2013; Fenelley, 2020). The weakest link theory underpins modern security protocols.

Weibull's Weakest Link with Multiple Flaws

The potential for multiple flaws is a unique feature of the Weibull model, which makes it more than ideal as a theoretical model for security issues. If more than one flaw exists in the material, the survivability becomes multiplicative (Zok, 2017), as shown in Figure 1.2.

Figure 1.2

The equation for survivability for a system with multiple flaws.

$$S = \prod_{i=1}^{N} S_0^{\mathrm{I}}(\sigma) \bullet S_0^{\mathrm{II}}(\sigma)$$

Each probability then reduces the other, overall reducing survivability probability. The crosswalk between security events and multiple failures begins to take effect.

The practical application of weakest link is the underlying belief that the area to fail is the weakest.

Alternative Theories, and the Flawed Fracture

The flawed fracture theory is an alternative to the weakest link theory. The flawed fracture model may better fit cascading events. Although never considered in published literature relative to cybersecurity, this theoretical framework represents a novel approach to security preparedness. The application of a fractured flaw approach has been postulated and examined to be better descriptive than the weakest link model. Research conducted in the 1970s in high-end

ceramic coatings showed the value of considering a fractured flaw type of failure over the most vulnerable or multiple weakest links (Batdorf, 1978).

The weakest link theory has been widely accepted and significantly impacted perspectives and information related to security. The weakest link theory has greatly influenced the approach and strategies. Beyond mathematics and the strength of materials, the flawed fracture theory did not exist in the literature. The tabletop participants represent insights into security issues inside and between each sector. The net implication for either theory is the same. The mathematical calculation would differ for material, but the results are the same for the qualitative application. The weakest link and multiple security issues have a multiplicative effect.

The nuanced approach recognizes that security represents organically symmetric systems. The security concepts protecting a business are a microcosm of those exact mechanisms protecting the large city as the levels and members increase. From this perspective, the systems have common responses and behave like homogenous material. Homogeneity introduces common failures. The same security paradigm failures on a small scale extend to the more extensive systems—standard training programs, certifications, and even teaching lead to the same shortcomings. The application of pre-fracture materials is an ideal fit. This study will evaluate the correctness of this assumption.

Theory Implications

The weakest link and fractured flaw theories contextualize the purpose of the tabletop exercise as well as the role of the participants. The tabletop exercise identifies security or response weaknesses in emergency response. Of specific interest are those in cybersecurity-related scenarios. As the exercise progresses, a forward-projecting case study works through. As the example goes, gaps in security posture are made apparent. The tabletop exercise works to

identify the individual strands within the overall security picture, much like the strands of material. The weaknesses of each security measure are compared and contrasted as to how they affect other sectors. The tabletop process addresses multiple vulnerabilities within a single exercise. Understanding how the individual fits within the overall model allows consideration of what factors are critical to success.

Theoretical Approach

Using a decision-theoretic approach, the weakest link presupposes failure occurs at the weakest point. The theory does not support weakness types or failure modes, just that the weakest link is the first to fail. The alternative approach postulated here finds that the same common flaw runs throughout the system, and the failure mechanics are interrelated. This interdependency is critical in strengthening the entire system. The fractured flaw theoretical value is that understanding the common failure (or fracture structure) supports the whole system. Transitioning to the novel application of the fracture flaw theory could fundamentally change the United States' security posture. Analysis of cyber attacks and tabletop exercises should reveal sufficient support to underpin the viability of the fractured flaw theory in security applications.

System of Systems

Overall, material strength is dependent on individual elements. From a multiple-level perspective, security is a system of systems (mirror of mirrors). Each organization comprises many departments, which could contain respective teams, eventually leading to individual employees. The recognition that the macro level theory likely extends into each sublevel is accurate for security considerations.

Cybersecurity Micro/Macro and Communal Theoretical Perspectives

The advanced cybersecurity study requires a generalized understanding of the micro versus macro perspectives. From an individual perspective, security includes cyber-hygiene activities such as password management, updating software, and minimizing the personal information shared on social media. The goal is to limit threats via authentication issues, proper authorization, data privacy, and system privileges (Shore, 2021). Authentication is the verification of who the person is gaining access to information (or systems) that they should be allowed to manipulate. Data privacy is closely related to authentication, authorization, and access issues but focuses on data protection throughout every cyber process. System access includes the rights to control authorization and authentication access and many other functional systems. System access is often the most important, especially in operational technology systems. The users with the highest system access are often the target of social engineering and spear phishing. The threats faced at the individual level are the same that attack each successive circle.

The next ring beyond the individual cyber account is the enterprise level. The enterprise-level examples include a single business, corporation, family, or school. These are family computers, family networks, work computers, work networks, school accounts, or even a municipality. For further context, for a family, this includes home routers, computers, smart televisions, security systems, and other intelligent devices. Similar cyber hygiene protocols protect users just as they did individually. However, new risks at this level include the threat of outsiders and insiders with direct access to equipment, the capability to watch passwords entered, or manual equipment manipulation. Children accessing a parent's computer may seem innocent enough, but using a work computer to work on homework or worse can introduce malware

through accidental downloads. At the workplace, malicious threats come from nosey coworkers or disgruntled employees.

The next level of cyber security interfaces is longer a two-dimensional model but more of a complicated three dimension set of concentric rings. The interconnection between overlapping computers starts touching many more entities. The home user or even commercial user almost always relies on an internet service provider to connect them to the internet. New parts, computers, components, and even software updates depend on various vendors. Business or enterprise networks introduce new undisclosed threats through malware or other exploits with each new network element. The vulnerabilities even include the interception of components via shipping from the manufacturer to the retailer. Counterintelligence and security professionals documented multiple cases of nation-state interceptions of components and systems enroute to intended targets (Mitchell, 2021). Outside individuals post threats in shipping, as well as insiders. The United States Government is aware of these threats and has implemented the Cybersecurity Maturity Model Certification (CMMC) (Russell, 2020). One of the main goals of CMMC is stabilizing the supply chain and attempting to address cybersecurity risks along the supply chain (Russell, 2020). The cyber macro universe perspective provides the system of systems communal view. Understanding the functional theoretical framework is critical to understanding the necessity for the tabletop exercise (Department of Homeland Security, 2003).

The future of cybersecurity is a zero-trust model where the overwhelming threat in each step is so significant that the previous step or process cannot be trusted (Shore, 2021). Zero-trust assumes that all inputs, whether hardware or software, are malicious and seeks to validate through external verification. Zero-trust originated circa 2011 and has grown in popularity, although it has yet to be adopted by the United States Government (Shore, 2021). The zero-trust

model assumes that even internal networks are compromised and looks to use third-party or multi-party verification techniques, including blockchain concepts (Alevizos, 2022).

Alternative Theories

An alternative theory for evaluating tabletop exercises is John Rawl's social contract theory, including those impacted by a potential crime or dispersion of lessons learned through the class of individuals. Inclusion or exclusion of participants could potentially cause them harm or provide protection. From a social contract perspective, the team members represent members of organizations which represent a greater community. From a social contract perspective, member should actively and appropriately participate in tabletop exercises.

Theoretical Harmonization of Cybersecurity Theories

The theoretical background directly impacts the construct of the tabletop exercise. The tabletop exercise works at the enterprise level and seeks to bring the overlapping spheres or circles of all the different individual businesses (Department of Homeland Security, 2003). The internet provider, the manufacturers, the users, and more all have interests in ensuring security perseverance. Whether the weakest link or fractured flaw, the tabletop allows the evaluation of the cyber risks that spread past the individual. The fractured flaw theory provides threats are more likely to come from across connections through standard failure modes.

Related Literature

Based on the theoretical map of utilizing the tabletop exercise to identify security gaps, critical infrastructure protection depends on selecting the proper individuals to participate in the activities. Alternative studies have supported participant-driven expertise based on participants (Kim, 2019; Mishra, 2014). The literature review focused on understanding the elements that

went into a tabletop exercise and the key features, critical attributes, roles, and knowledge brought into successful training.

From a big-picture perspective, safety, security, and resiliency are the co-linked problems. The security of each often depends on the other links in the chain. A perfect system on an isolated portion of the complete picture fails to provide security for them all. The current prevailing theory in security is that the overall protection of society depends on the weakest link. The weakest link theory is particularly true compared to cybersecurity-criminals will poke at each portion until they can find the weakest link. However, the flawed fracture theory is a better fit since each piece of the overall system represents a system of systems or subsystems. The overlapping of individual enterprises from a macro perspective exponentially increases threats.

Cybersecurity adds a new layer of complexity to old problems. The number of people, companies, and organizations involved inside each system is higher than in any other area of traditional crime or protection. The plans include component manufacturers, integrators or assembly, software designers, operating systems, network operators (internet service providers), procurement, installation technicians, security personnel, and more at the component level. At the next level, these devices form subsystems with many of the same elements and function as subsystems to even more extensive networks. The layers and layers of systems complicate the overall protection of the entire global system. To deal with the unique problems of cybersecurity, a culture has developed around cybersecurity unlike any other.

Cybersecurity culture utilizes checklists, best practices, deception, software, monitoring, and prevention. The system's most common failure and weakest point are often the ones involved. Significant training and effort develop a cyber hygiene culture in the workforce to recognize social engineering efforts, spear phishing, phishing, and abnormal network behavior.

Ultimately, most actions become marginalized by security experts to checklists and monitoring software.

Tabletop History

Medical and emergency planners have used tabletop exercises for many years. Early tabletop exercises focused on a single agency. Law enforcement or government agencies were the only participants. Tabletop exercises became a standard method for dealing with emergency response issues following the September 11, 2001 terrorist attacks (Department of Homeland Security, 2003). The National Incidence Management System (NIMS) training required for emergency responders provides the direction of tabletop exercises. NIMS states that "emergency management/response personnel should also participate in realistic exercises-including multidisciplinary, multijurisdictional incidents, and non-governmental organizations (NGO) and private-sector interaction-to improve coordination and interoperability" (Department of Homeland Security, 2003). The NIMS training further suggests that stand-in actors play all needed roles in a training event (Department of Homeland Security, 2003). The tabletop execution includes participants representing the emergency response actors and the antagonists as the primary actors. Planners and observers prepare the scenario and enforce the training rules. The inclusion of the right members can mean improved preparedness for all involved. NIMS training recommends acknowledging and filling excluded industrial partners with a stand-in actor (Department of Homeland Security, 2003). NIMS training is silent on how to handle overlooked participants. In the recent exercises conducted by the Army Cyber Command, the lack of guidance on who to invite became apparent. Planning new events is also challenging as there is no common starting point. Research should document who to ask within an organization, skill level, and career level.

Tabletop Execution

Scenario developers (or planners) organize the event and often develop the scenario. Scenario planning may be done independently or with help from the participants. A team of data collectors will often record interactions and results during the procedure. The scenario developers and data collection teams are law enforcement and the government (local or federal).

Participants - Participants often include emergency planners, emergency managers, and politicians. Recent cyber planning events and tabletop exercises have included infrastructure and commercial sector participants. Unfortunately, including infrastructure or commercial parties is sporadic without strategic or tactical considerations. Practitioners are concerned that whole infrastructure sectors are not participating.

Antagonists (Cybercriminals) – Antagonists are criminal cyber attackers that could be terrorists, organized criminal elements, terrorists, or state actors. The antagonists can include pirates, foreign state hostiles, militant-based violent extremists, political motivations, and financially motivated terrorists. The causes or triggers vary greatly. The only uniformity between the various groups is the mechanism of a cyberattack. Cybercrime provides the promise of anonymity. The probability of detection and capture is significantly lower than in traditional crime. The amount of disruption and chaos is disproportionate to the effort required.

A senior volunteer professional usually plays this role in a tabletop exercise. Depending on the scenario layout, they can often respond in a predetermined set of actions based on the initial planning layout. Depending on the configuration, they may be sequestered from the victims or in the same room. Other variations include the antagonist's entire role being pre-scripted, wherein the event planner reveals information sequentially as if it were in real-time.

Tabletop Rules - Rules of engagement from each participant often include responses based on historical precedent, procedure-documented response, documented capability, and standard operating system. Security professionals identify vulnerabilities when a participant becomes stuck. A reasonable answer provides the means to facilitate the exercise continuing forward. Traditional tabletop rules also limit the response to real-world capabilities. The team's responses cannot exceed their authority or powers. The rules also ensure that all participants play fair. A real-time actor may play the antagonist and interactively respond to the scenario, depending on the setup. A typical practice for the antagonist is a proven successful attack utilizing the means and methods proposed in the response. As part of preplanning, the antagonist may independently walk through all proposed attack vectors or inject with the planning team. The planner evaluates the proposed options for validity. The planning team also ensures that their opponents stay independent from the participants.

Tabletop Planning - Although the planning and preparation of an event are enormous, there is little to no discussion on who to invite and include. An anecdotal review revealed several instances of identifying the level of personnel in a tabletop exercise but offered little guidance on who to select. For example, the Army Cyber Institute provided a three-tier stratification of attendees, senior executives and chief executive officers, mid-level managers, and field level managers. Mid-level managers provided technical knowledge in the Jack Voltaic exercises, but the technical experts were at the lowest level. In one study, the senior leaders failed to participate, which affected the ability to make real-time decisions in actual events. Summarizing the findings from the literature, the only positive conclusion is that including multiple levels of an organization produced the most favorable results.

Typical Tabletop Participants

The scenario developers (or planners) organize the event and often develop the scenario. Scenario planning may be done independently or with help from the participants. A team of data collectors will often record interactions and results during the procedure. The scenario developers and data collection teams were law enforcement, government officials, or even hospital system staff (local or federal).

Participants often include emergency planners, emergency managers, and politicians. Recent cyber planning events and tabletop exercises have included infrastructure and commercial sector participants. Unfortunately, including infrastructure or commercial parties is sporadic without strategic or tactical considerations. Practitioners are concerned that whole infrastructure sectors are not participating.

Beyond the groups that typically participate, the last several years have seen a new set of participants, a legal team. Lawyers from each organization have weighed in, limiting information sharing or aid offered. The legal interactions have added an exciting impact to some of these exercises. The inability to have government sectors assist private businesses depends on local, state, and federal law, which often depends on what has happened and the local response.

Scenarios

The timing delays caused by legal reviews play out in scenarios just as in real life. Recent advice offered by the Army Command recommended moving the legal evaluation into its separate exercise [although beyond the scope of this analysis, the impact of separating the frustration, advice, and delay from an actual event and its effect should be the focus of future research]. The legal evaluation adds an additional dynamic by delaying the exercise and slowing

decision-making. The value is the process realism provided by including legal. Most agency or enterprise actions receive legal review before action regardless of the expediency of the issue.

Cyber Security

Cyber security is only one of a host of hazards that could be the focus of the tabletop exercise. However, cyber security is unique in providing a remote access point to an asymmetrical attack unavailable until recently. The promise of anonymity also attracts those who would otherwise not engage in criminal acts. Cyber attacks also represent the fastest-growing risk in the United States. The attacks are increasing, and the surface area and means of attack constantly change. Executive Order 13231, the Cyber Security Enhancement Act of 2002, and most recently, on May 12, 2021, Executive Order 14028 significantly increased the cybersecurity measures required to protect Critical Infrastructure and Key Resources (CIKR). The following background provides needed information to aid in the research and advancement of identifying the appropriate participants.

Historically, cybercrime did not exist, and historical methods are ineffective at preventing cybercrime (Anglin, 1999). One of the unique aspects of cybercrime is the wide range of individuals, terrorists, and even governments engaging in cyberattacks. The wide range of antagonists causes problem-oriented policing to be non-effective in preventing crime (Vito, 2015). Addressing the root cause of cybercrime is impossible because no single set of root causes exists. Greed, state-level hostility, and terrorism are not likely to have a long-term solution or rational reasons.

Cyber Security Scenario Participants

The literature identifies no specific set of antagonists for participation in tabletop exercises. The host organization, event planner, or other volunteers are the bad guys. Tabletops

focus on the participants in the practice of good actors working to prepare and recover from an attack. Much of the scenario preparation develops the script for the potential criminals. One variant uses an active antagonist with a preestablished set of actions.

A 2011 study concluded that 431 million adults experienced cybercrime, and 14 are affected every second (Cybercrime, 2011). Cyber-attacks are broad and come in many forms, including phishing attacks, ransomware, and physical and operational attacks. Research has shown that 22% of all data breaches involve phishing attacks, but 82% of reported security incidents (Barker, 2021). However, most malware replicates through phishing attacks 94% (Barker 2021). Based on the data, most cyber criminals attack at the individual level and then spread the enterprise into co-linked macro systems. The attack may come via multiple means or attack vectors.

Severe operational technology attacks tend to cause physical harm. Some of these physical attacks have injured and killed its victims. Recent examples include manipulating global positioning signals (GPS) to cause collisions among marine vessels and airplanes to overshoot runways (Paul, 2019; Woody, 2017). Another example was the overloading of a shipping vessel in the port of Brunswick, Georgia. The automated shipping containers were maliciously affected to overload one side of the ship, causing it to capsize as it attempted to leave the port (Paris, 2019). Cybercrime is real and poses a real risk to the health and prosperity of the United States. The difficulty in detecting that a cyberattack has occurred is more insidious than the number of attacks.

The attack vector is critical as it identifies the first area of attack, and from there, the consequences, communication, and impacts flow from micro to macro. The initial attack vectors come from probabilistic data on recent episodes. Recent exercises have tended to use the

individual as the initiating compromise. The malware or intrusion uses authorization or access vulnerabilities from the initial attack to cause further havoc. To ensure training realism and to help participants learn, several turns may go by before the participants are allowed to react. The goal is to train the emergency responders on how long it takes to detect an attack. The scenario often walks through a criminal timeline so the team knows how late they may respond. In the literature, scenario development utilizes real-world examples. Initial attacks may have little to do with how the exercise goes. Several examples had second or third injections that had a much more significant impact than the initial attack. The effect of the public response to a minor misinterpreted inconvenience can snowball into a much more inappropriate and harmful fear response. In the end, the scenario planners design the exercise. Hence, the participant team learns how to respond to a similar event and can work through the possibility of affecting the outcome.

Historically, cybersecurity focused on the Information Technology (IT) portion of the risk. IT concerns the network, data, email, electronic communication, etc. The other part of cybersecurity is Operational Technology (OT). OT represents the interface with the physical world. The risk with the growing OT world is that they represent an easy gateway into the IT portion of the network, but more importantly, the OT represents the real threat of past stolen information (Loeb, 2016).

IT is the internet, email, traditional computer, and other communication technology. IT includes software but only limited hardware. IT encompasses the messaging between computers, machine language, and operating systems specific to central processing units, mainframes, and servers. A few gray areas exist between operational and information technology. Examples include compromised data cables and devices that do internal calculations with the software but

are not accessible by humans (this would be like a pressure gauge that reads an answer in volts through an ohmmeter that uses temperature and flow rate to derive a resulting solution).

The rise of operational technology and connected devices has opened new avenues for potential harm. OT has increased the possible means of attack to include every intelligent device. The current connected world is growing exponentially. Operational technology represents a physical threat to life and safety (Barker, 2021). The limit switches on trains, the chlorine levels in the water system, and the discharges from chemical stacks are all controlled by OT devices. The supervisory control and data acquisition (SCADA) system that runs boilers at the Central Intelligence Agency to the local water treatment is vulnerable to attack. The SCADA systems operate in nearly every system in the United States, including traffic lights and power systems (Erickson 2019). The Stuxnet virus demonstrated that a cyber-attack focused on OT could more than temporarily shut down operations but cause irreparable damage to equipment (Balford, 2013). This attack can also extend past destroying equipment to harming citizens and causing terror and fear. Light bulbs, front doors, cameras, and the future of smart homes and self-driving cars have only opened a new world of potential threats.

Unprotected operational technology assets represent the easiest way to attack a physical target with the least effort. Anonymity, remote capabilities, and increasing applications will only cause operational technology cybercrimes to continue to rise. A second point discovered through analysis of the issue is that cybercrimes usually take two forms: a cyberattack using a system vulnerability like an unsecured network port or a human exposure. A human vulnerability could include dropping a USB thumb drive on someone's desk to get them to install malicious code unintentionally or sending a phishing email and tricking them into clicking an unsafe link. The analysis also showed that targets are related to IT, network connections, software, computers,

and OT, the sensors, and instruments that interface with the real world. For this paper, IT and OT are the same targets for cybercrimes.

Each year has seen exponential growth in the number and sophistication of cybercrime. For example, phishing saw a tremendous spike following the onset of remote work with the COVID-19 Pandemic. The number of counted phishing attempts averaged right under 50,000 from August 2019 to March 2020. The second week of March 2020, the COVID-19 pandemic response marked the beginning of remote work and school for most of the United States. In April 2020, phishing attacks jumped to 65,000; by May, there were over 100,000 in a single month (Barker, 2021). From June 2020 until the present, the current average has been 150,000, with more added each month (Barker, 2021).

Ransomware trends are growing among municipal and state-level government agencies (InfraGard 2019). Ransomware attacks at hospitals, schools, cities, and more cybercrime target softer targets related to industry and critical infrastructure are exponentially growing. Although less common, these have even targeted law enforcement agencies (Walker, 2021). The investigated attack against the South Carolina Law Enforcement agency led to unauthorized access to law enforcement data. The agency recovered and restored the data only to be attacked a few months later (C. Walker, SC Law Enforcement Division presentation, January 6, 2021).

During a ransomware attack, the criminal encrypts the operating system or related files. Cybercriminals release the encryption keys upon ransom payment (Monika, 2016). Other data breaches rely on covertly gaining access to cloud-based or local servers and utilizing the network to attack. In other cases, cybercriminals use a hybrid combination of methods. In 2020, the most potent and most dangerous attack in the United States took a variation on the server attack. What appeared to be a typical ransomware attack was a cover for one of the most damaging attacks in

recent history. The Solar Winds breach allowed access to the tools to prevent cybercrime (Walker, 2021). Russian hackers stole the source code for Nessus scanning software. Cybersecurity professionals use Nessus to make sure there are no network vulnerabilities. The hackers then reworked the original code to include malicious software. Using the tool to protect the network only spreads the virus, creating new vulnerabilities. A large fear is that ransomware attacks will evolve into attacks with goals of disruption and violence instead of the status quo of financial piracy.

An additional form of attack can occur with a man in the middle type of attack. In this scenario, the maleficent actor covertly inserts themselves in the middle. The South Carolina Law Enforcement Division survived such a ransomware attack only to be attacked a second time. The second attack on the South Carolina Law Enforcement Division also affected the Georgia Bureau of Investigation (Walker, 2021). The underlying value of this attack was that both agencies held two tabletop exercises to ensure this type of attack did not occur. The tabletop planner left out the internet service provider (ISP). No one played the ISP in two tabletop exercises (Walker, 2021). The attack on the internet service provider led to the public release of all the private information of law enforcement in both states (Walker, 2021).

Cyber Defense Strategy Overview

Cyber defense strategies and capabilities are essential because of the potential to impact response and are directly related to security strength. Cyber hygiene models and cyber education prevent most simple attacks against computer systems at the individual level. Cutting-edge research discourages the historical approaches of "perimeters are usually protected by security measures such as firewalls or intrusion detection systems" because they are less effective (Alevizos, 2021). Cybersecurity historically used antivirus software, firewalls, and intrusion

detection to protect IT and OT to prevent attacks from an individual perspective (Alevizos, 2021). Perimeter-based security has been replaced with a digital identity-based perimeter and actively uses multifactor authentication (Alevizos, 2021).

Other recent changes in cyber defense have also come in the form of target identification. Idaho National Laboratory has prioritized the most at-risk systems (Freeman, 2016). Advances in cyber security have identified the protection of the most critical aspects of digitally backed infrastructure as the only thing to be protected. However, little direction exists in identifying those elements. When provided, the ranking information is single-client specific. There is no detailed guidance on prioritizing digitally enhanced features when examining communities or communities of systems. The ability to prioritize the most critical attack vectors would provide insight into what must be protected first. Identification would prioritize funding, monitoring, and even signal potential attacks. Ideally, planning and preparation for an attack happen long before one occurs. Knowing what to protect on an individual and communal basis is necessary to identify and protect all vulnerabilities.

Currently, there is no guidance on planning tabletop exercises (TTX), identification of participants, or methodology for ensuring the entire Area of Emergency management professionals use tabletop exercises to evaluate performance on prepared written scenarios (Wendelboe, 2020). Tabletop exercises defined by the Department of Homeland Security have facilitated group analysis of an emergency (Department of Homeland Security, 2003). Tabletop exercises measure existing programs and decision-making performance on resilience in the specific scenario, varying from large-scale to small single-facility events. Tabletop exercises are also used to assess the readiness of Incident Command systems in the United States and can cover any subject or design. The Homeland Security Act of 2002 and Executive Order 13010,

Presidential Directive 7 (2013), require identifying critical infrastructure by government agencies to protect them. Critical Infrastructure and Key Resources (CIKR) exist in many forms. Private companies own some CIKR, while government agencies own many others; in each case, the safe operation allows the continuity of normal operations.

Alternative cybersecurity modules focus on the human element's weakest link in all systems. Humans cause failures, and improvements remove or train the human loss. Removing the human aspect would be effective if the lowest link were the correct controlling theory. However, removing the human element does not remove all the attack vectors. Regardless of the initiating step, the overlapping interdependency means a failure in one section causes the potential for additional shortcomings. Assuming they all come from humans in the system is not adequate.

A cascading event is a series with a single initiation or multiple initial events. Literature showed that the most commonly deployed model was a series of initial attacks followed by scenario injections as the exercise progressed. The more straightforward scenarios examined broken equipment or a failed system. Most systems are much more complicated, and an actual terror attack is more likely to be accompanied by multiple assaults. A single source attack versus cascading impacts is similar to the difference between portfolio and asset analysis. A portfolio analysis is a high-level analysis that compares how systems of facilities work together. This analysis should consider the portfolio comparison a concerted, complicated scenario. An asset-level analysis would be the individual components within a more extensive system, such as losing printers or air traffic control screens. From a risk perspective, the portfolio analysis is more representative of the real threats posed by cyber terrorists. The Jack Voltaic exercises conducted by the Army Cyber Institute showed that a sophisticated cyber opponent could cause

potentially catastrophic consequences even though isolated, simple series of attacks (Mitchell, 2021).

A feature unique to cyberattacks is the potential to weaponize a facility against itself, the community, or other buildings. As previously covered, the operational technology attack allows the attack surface to extend into the real world. The ability to use a co-located or nearby facility as a weapon is a real risk. A standard hazards assessment includes risks posed by nearby facilities. The most straightforward sorts of OT attacks were on printers. Cybercriminals can print propaganda and steal sensitive information. In the last ten years, the ability to cause the printer to overheat and cause a fire has become a reality. In 2020-2021, new threats emerged regarding the remote use of intravenous pumps in hospitals, home alarms, and even remote driving of Tesla vehicles. Criminals can use these exploits to carry out more significant crimes.

Operational technology threats open the door for tabletop planners to develop various scenarios. The Stuxnet virus used against Iran caused the plan to self-destruct. Scenario developers evaluated the capability to poison an entire town using existing water treatment facilities. Using chemicals used to clean or trim the acidity/basic nature of the water can be overloaded to poison the population. No additional chemicals are needed. Criminals living anywhere in the world pose a potential cyber threat. The ability to recognize that the cyber threat extends to every device and even those nearby further complicates the ability to protect people and facilities, making tabletop exercises critical.

Conclusions from Literature Review

Based on the literature review and mapping with theoretical models, a fundamental understanding is that the tabletop participants must provide quality information sufficient to identify either an internal security flaw or a security flaw between interfacing organizations.

Tabletop exercises are most effective at identifying security flaws between organizations. An additional conclusion is that the same flaws often exist across organizations. The security risks are not unique to the weakest member of the security chain. The defects found in the proposed weakest link exist in most group members. One difference observed from the literature is that larger organizations have more staff and resources. Additional research may shed light on whether the capability and resources to respond to an attack underway prevent further issues or if the attractiveness of less protected assets causes their target value to increase.

Tabletop Factors

Prior research found that members who had previously participated in tabletop exercises improved the exercise (Agboola, 2013). Participation in more than one event helped participants improve their performance. The study limited previous involvement within the past three years and included 174 participants (Agboola, 2013). The study also found no link between size, training, education, status, or years of experience (Agboola, 2013). Several other tabletop exercise designs completed the same scenario with different participants. The most interesting tabletop exercises were repeated within the same state. No significant deviations were noted from each exercise (Araz, 2013). However, the research with the highest participation looked at the same scenario with multiple samples. This research controlled the scenarios and limited the repetitive tabletop exercises to participants within a single hospital system (Araz, 2013). Extrapolating how that may impact members from different organizations is not possible.

Related Literature

Current literature highlights the gaps in the macro view of cybersecurity systems. The challenge for tabletop exercise planners is developing effective practices depending on realistic

scenarios. Planners have to identify appropriate participants. Preparedness experts have identified the need over time to be able to prioritize and rank risks, issues, and facilities. Prioritization allows the intelligent allocation of funds and resources. Although this has yet to occur with participants, multiple similar efforts are complete. Examples of parallel research include prioritizing CIKR sectors (Fisher, 2010).

The material sciences world adopted the switch in theories from the weakest link to fractured flaws for more than 70 years. Advances made with new technology, higher power microscopes, and scanning microscopes shed light on material failures or fractures. Those modifications to the base theory now account for the current understanding of material sciences. The theories also effectively predict when and how elements will break.

The related literature to fractured flaw mechanics may yield direct applications to security applications. One of the most significant advantages of the fractured flaw theory relative to structural mechanics is its ability to explain how materials interweave from atomic, molecular, ionic, and covalent bond perspectives (Lawn, 1993). The more complicated theory examines how the interactions of electrons and atoms lead to nuclear bonds and crystal structure. This structure then makes up the whole of a substance, which sees the external forces that eventually cause the material to break. Extrapolating the fractured flaw theory into the cybersecurity world generates the identification of additional correlations. Regardless of the users, the cyber systems fail into the same sub elements. The electricity runs through every component, the components in every machine are similar, every device runs identical software, the software users all have similar security postures, procedures, and arrangements, and will all suffer from similar modes. A brief overview of related literature transposed a significant body of work into security applications.

Significant quantitative research provides the failure mechanics for solids and the means and methods to strengthen the materials. Future security research will benefit from evaluating strategies to crosswalk this information. The related literature review shows many approaches to improving the overall strength of a system. The comparison from casting flaws to missing participants. Research also showed that the environment that houses a material could have significant impacts. Caustic stress corrosion cracking causes austenitic stainless steel to have a failure mechanism that does not occur in any other scenario. A security corollary exists between Radical Islamism, Militia Based Violent Extremism, or cultural influences between material environment data. Environmental factors increase the fracture or failure rate of materials, much like extremist behavior increases terrorism and crime.

The sponsoring agency's influence on the outcomes is another consideration for tabletop exercises. Several sources evaluated the impact of the sponsoring organization. A large body of knowledge exists related to sponsorship influence in sporting arenas. Based on the data collected, the sponsor did not impact the results when supporting multiple teams, nor did the sponsor participate (Davies, 2006). In tabletop exercise development, the sponsoring organization nearly always participates. The Army Cyber Command-sponsored events have focused on force projection sizing. There is reason to believe that this may have impacted the outcome.

Related to research question three, does the sponsoring organization affect the outcome of the exercise? The research literature review expanded to look for similar cases of potential bias. Research relative to the medical community looked deeply into the tobacco industry and the impact tobacco sponsorship had on expert outcomes.

Summary

The researcher retrieved roughly 42,847 articles related to cascading events in June 2022. The growing reason for concern is that a minor undetected attack can have a much broader cascading effect. The ability to understand and describe the risk well is still in its infancy. Current research is based only on probabilistic information, confined to coding and binning original typography. Tabletop exercises are the only method designed to handle cascading scenarios.

The literature research provides a basis for understanding what is known relative to a subject. Countless TTXs have analyzed an accurate set of all hazards. The researcher could exclude or include subject matter or scenario-driven exercises when reviewing the literature. As the researcher gathered the related literature, it quickly became apparent that most scenarios had little to do with selecting participants. The sparsity of literature in any sector on participant selection made it easier to keep all research on participants regardless of the scenario. Cyber-attacks can impact upstream and downstream customers, whether criminal, terrorist, or war-driven. The impact spread in cyber attacks is similar to many of the medical or postulated medical Pandemic exercises reviewed. They all have consequences that extend beyond the initial incident.

Historically, tabletop planners do not spend much time trying to identify participants. The emergency preparedness community recruits for exercises; only those volunteering attend the TTX. A substantial limitation of historical activities was the failure to identify missing groups. In some cases, this information may be available from videotaped planning recordings. No other organization had that type of analysis.

The planners can affect the training through numerous means. The TTX planers can physically separate participants by industry, team, and city. The researchers use separation to control communication flow. The more realistic a scenario, the better the outcome and the more important having the correct participants become.

Literature Research Question 3:

Were there any interesting findings that indicate issues with team identification?

Several themes popped up in the literature that may indicate the tabletop is not producing valuable results due to missing participants. The exercise intends to make findings of inadequacies or gaps in responses. Although nearly every activity can help review policies, procedures, and even decision-making, the lack of new issues or repetition of only known old issues may help judge the success or failure of participant selection. Emergency room and medical exercises identified the lack of new findings. The lack of quantitative measurements and the repetition of previously identified problems were the only findings from medical practices (Dausey, 2007). Non-value-added results could be indicative of similar significance issues with other studies.

An additional finding was that a few included impacts across multiple sectors out of the 16 Critical Infrastructure sectors. The first significant examples were conducted in 2018 by the New York Fire Department and the Naval War College. Fifteen of the 16 industries comprised the exercise (Pfeifer, 2018).

In the literature review, the zero-day vulnerabilities provide the best evidence linking the weakest link and fractured flaw theories. Many cyber attacks utilize zero-day vulnerabilities. A zero-day vulnerability is a failure, flaw, back door, or unintended function of a program that cyber criminals may exploit. The term zero-day describes that security professionals discovered

the vulnerability. The medical analogy would be a ‘patient zero’ for a new virus. When criminals maliciously use a zero-day vulnerability, all parties could be victims. The Stuxnet virus, for example, contained multiple zero-day exploits, but the virus specifically targeted the operational technology used by Iran (Balford, 2013). The Stuxnet virus utilized a known worm virus to spread its code. The Stuxnets used zero-day exploits to damage a specific set of centrifuges (Balford, 2013). The same application could have easily damaged any other item everywhere, but Stuxnet had a particular target. A terrorist utilizing a zero-day exploit is just as likely to attack the weakest link as the strongest. The precision required to create a highly targeted weapon is more difficult than one to cause generalized, widespread harm.

From a global security perspective, the fractured flaw theory has applications outside of cybersecurity. Changing the perspective on security from the weakest link to the common failures approach changes the paradigm in which the security community sees risks and threats. More advanced users are likely already making this change; the theory dictates that similar flaws may exist across the material or system when discovered anywhere. Advanced security personnel share information, however limited, and all seek to strengthen once criminals use a vulnerability or new attack vector. The power behind the fractured flaw theory is that it changes the perception of threats. The fracture flaw theory improves survivability by addressing the elements that go into the structure (Lawn, 1993).

Conclusion

Regardless of the data source, scenario, or those involved, the lack of an organization with effective representation in an exercise or preparedness presents a fatal flaw. The considerations or concerns of that organization look like a missing puzzle piece. The lack of a team member represents a complete missing link in the weakest link theory. However, going a

step further also means a critical flaw in a material from a fractured flaw perspective. Failure to include a link in the system creates a gap. The combination of theories to propose a new working theory based on the macro and microstructure that addresses common failures lays the foundation for the following research phase.

The scenarios generated the most findings, and changes have included major cyberattacks in densely populated cities (Pfeifer, 2018). The CARVER assessment tool originates in the U.S. Special Forces, dates back to WWII, and evaluates the Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability (Bennet, 2018). Understanding the CARVER impact summarized in resiliency and ease of target acquisition are significant components of current national security missions. Reviewing the literature revealed limited information on determining how / who to include in tabletop exercises. There is no guidance for the tabletop planner on who has to participate in the tabletop exercise. The data is precise in that greater participation adds value and uses a stratified approach in using employees at multiple levels.

In general, multiple studies recommended limiting participant size based on the complexity of the scenario but also acknowledged that realism is lost as actual events often include more participants than allowed (Dausey, 2007). No definitive literature impacted missing participants, although NIMS training recommends that stand-in actors play missing participants Department of Homeland Security, 2003). On a positive note, the literature showed that any sizable team was good enough to learn from, regardless of the type of drill. The difficulty in gathering attack or crime count data has also highlighted the need to conduct qualitative surveys with cyber professionals and potentially include willing cybercriminals. Literature specific to tabletop exercises did not consider increased risks due to participation.

One of the major research questions was the impact that sponsoring agencies' agenda had on the outcome of the training exercise. Related literature noted that the sponsoring agencies' plan likely influenced exercise outcomes depending on how the agency participated. Related and conflicting research also exists on whether or not the sponsoring agency makes a difference. Studies in the tobacco industry showed an impact, but sponsorship in the sports industry made no difference. The literature conflict provided insight into the appropriate framing of the future research question. Based on the previously conducted tabletop exercises, participating agencies often sponsor the ones planned for the future. The agencies have an agenda, and verification that this impacts the results would be a beneficial insight into preparing and conducting tabletop exercises.

Another picture arises by combining the various theories with the related literature data. The more extensive networks and interlinked systems are what need to be protected. However, looking at the data, the attacks appear to be the highest at the individual level and then cascade from the individual to the enterprise to the more extensive macro community. The importance of the failure mechanism highlights the likelihood of fractured flaw theory providing a better description of reality. The underlying fact that the individuals who attend similar training use similar equipment on shared networks generically means that if one has a flaw (much like the recent Nessus breach), it extends across most members. The failure occurs not in the weakest member but in the targeted part of the macro system. Nothing in the literature would indicate that the targeted individual would have to be strategically chosen and would be akin to a crime of opportunity.

CHAPTER THREE: METHOD

Overview

This study examined the impacts of conducting tabletop exercises in preventing cybersecurity events. General Petraeus has repeatedly stated that cybersecurity is the most significant national security threat. The primary method the security industry uses for preparedness among multiple integrated systems is the tabletop exercise. The implications of not having appropriate representation from all integrated partners involved in a tabletop exercise, the act of participating, and the level of involvement affect the exercise's efficacy of the exercises. The effectiveness of the training directly impacts the overall security of the community of all members. An unprotected portion of a security profile renders all other security features meaningless. Compared to physical security, a gate and fence system represents a security barricade for the procedures. A three-part fence without a gate provides only a decorative feature. Failing to include the correct participants renders sophisticated planning, programs, investments, and efforts pointless, much like a three-sided gate. Leaving integrated components out of the overall assessment fails to improve security.

This research aims to understand how to identify and select the correct participants for tabletop exercises. Risk assessments consider an all-hazards perspective; a unique challenge in cybersecurity is failing to identify all vulnerabilities. This study aims to develop a framework that allows a vulnerability perspective. The researcher will elucidate the risk of failing to identify sectors or participants, missed sectors, the false sense of security caused by omissions, and other dangers through detailed procedures, research design, and analysis presented. The researcher believes that applied research will improve cybersecurity by improving the effectiveness of tabletop exercises by creating solutions to an immediate problem (O'Leary 2005).

Although much effort has gone into tabletop exercises, little analysis on the effectiveness of event prevention or the consequences of even participating, the tabletop exercise allows participants to drill scenarios and walk through them so they can understand how each different sector will respond. The inter-agency interaction alone often leads to significant, unexpected discoveries. However, the implications of leaving needed team members out has led to the potential for unanticipated vulnerabilities. Participants often have a perceived level of preparedness in stark contrast to their actual preparedness, which is an unintended consequence of participation (Nam, 2019).

Another concern is that even participating in these events can flag participants as high-value targets. Limited research has shown that fears over participating prevent participation (Hatzivasilis et al., 2019). The literature research has identified this as a potential concern. Opportunistic attackers are likely to attack opponents randomly, whereas all other actors are likelier to attack specially targeted victims (Ulven, 2021). The final problem is that the sponsoring organization's goals may trump the security of the objectives of the community participating. The research methods will investigate who participated in recent tabletop exercises.

Design

The qualitative study utilized data and research to examine past exercises to identify critical factors regarding tabletop exercises impacting security improvement. Based on previous research, the participant selection and the decision of whom to include and exclude profoundly impact the tabletop exercises' effectiveness. The research design examines participants' experiences inside of the tabletop exercises. In the future, it may be possible to compare tabletop exercise results against real-world impacts. Where possible, any overlaps of participation

preceding an attack were for comparison. Exercise comparison against real-world attack data and evaluation of actual impact would be the ultimate goal. The researcher will explore the potential risk of participating and being flagged as a high-priority target.

Based on literature reviews, there is a massive gap between the actual intent of emergency response planning and the desired outcome for some participants. The gap may be even more true for non-sponsoring organizations. The smaller agency participates looking for help, only to walk away with their vulnerabilities exposed with no additional support or guidance on how to close new gaps. A secondary challenge is this information is then publicly shared and discoverable through open sources. Although smaller agencies receive invitations to participate (or even participate), they may walk away with a false sense of security.

The research methodology is a qualitative grounded study to identify critical factors impacting security improvement following tabletop exercises. This approach will allow the documentation of the impacts of team selection omissions, the consequences of participation, and the effect of the sponsoring organization's agenda. Study participants provide their first accounts, providing new theoretical concepts. The applicability of the qualitative study and approach is the most appropriate research design. The research plan outlines the key steps to capture often lost information through the methodology, participants, procedures, analytical methods, and ethical concerns.

Methodology Selected

A qualitative study is necessary to explore the participant's perceptions and experiences in a tabletop exercise (Stake, 2010). A quantitative study was not viable for several reasons. The data relates to perceptions not captured, and additional issues relate to extremely temporal information. Tabletop planners rarely capture detailed notes on interworking of drills. A

secondary factor impacting the limitation of quantitative analysis is the overriding need for the data to disappear so that it was not available to malicious actors. An ethnographic approach was inappropriate as cultural norms or behaviors have a limited impact on the research topic. The research will use surveys as part of the descriptive research design but will lean on qualitative interviews. A qualitative approach is the most appropriate based on the need for perceptions and the impossibility of conducting quantitative analysis (Creswell, 2003).

Grounded Theory Methodology

The qualitative study utilizes a grounded theory approach. The date is encoded to provide the basis (or grounded) approach to insight. Surveys and interviews both used this approach in the analysis of the data. The research information compares to the other two overarching theories behind security breaches. The commonly held one is the weakest link. The alternative theory proposed by this research is the fractured flaw theory.

The grounded theory approach guided the research methodology to evaluate the postulated governing theories. The grounded theory shows coding information, generating field notes, analyzing data to compare to the proposed theories, and using the data to interpret the theories. In addition, the postulated theories of the grounded approach allowed the researcher to seek insight into new or alternative theories not considered at the onset of this research.

Research Questions

RQ1: What is the impact of having the wrong or missing participants in a tabletop exercise?

RQ2: What is the consequence of participating in a tabletop exercise? Does this cause additional risk?

RQ3: Do the agenda, goals, and objectives impact the outcome of the tabletop exercise's effectiveness?

Setting

The research setting was the United States and included United States-based emergency response personnel and companies. The researcher considered including Canada and Great Britain, but narrowing the focus to the United States was preferred based on the literature review. The literature review did show that the United Kingdom openly shared more intelligence related to cyber-attacks and maintained that information publicly for a longer time than any other country. Additionally, the research included as many participants as possible in the Jack Voltaic series of tabletop exercises and events planned for two months following approval of the dissertation topic. The Jack Voltaic was a fictional name given to a series of exercises that examined cascading terror events across the United States led by the Army Cyber Command.

Surveys

Each participant will take the survey in whatever location was convenient. The survey format was fillable on multiple electronic formats, including phones, tablets, and computers. The research did not control the electronic platform as convenience will likely affect the response rate. The survey captured the attribute data of name, organization, size, and organization type, which could be left anonymous. The overall results considered the impact of anonymous responses based on their overall proportion of responses. The researcher binned the organization's size into less than 100, between 100-500, and greater than 500. Then, the researcher categorized the respondents as commercial, local government, state government, or federal government. The final attribute question was related to tabletop participation. The researcher then split tabletop exercises into emergency preparedness or cybersecurity exercises. A negative response in both disqualified the survey from further use.

The survey included four more specific questions relative to tabletop exercises. The last

four questions sought a macro level to elicit a general community feeling and identify candidates for follow-up interviews. The first question asked, “Was the exercise beneficial or your agency/company?” The second question was specific to the exercise and sought beneficial experiences. This question is essential as the tabletop exercise may or may not add value if not appropriately focused. A controlled variable or assumption of this research is that the tabletop is generally practical based on years of research if it includes the appropriate participants. This question ascertains the quality of the tabletop exercise in general without regard to the participants. The first two questions seek to summarize the overall value of the process. Before testing began, the researcher expected positive responses to these questions. The third in-depth question aims to understand participant issues; “Did the exercise miss participants, or were stand-ins used?” elicits missing actors. NIMS training and common practice allow for stand-ins if missing. The planner identifies stand-ins before an event and others in situ as gaps arise. The overall goal of using stand-ins is to keep the exercise going; however, there is concern that the agency/sector missing does not benefit from the exercise, and any response may be invalid or even impossible. The final in-depth question was, “Do you know of anyone being attacked closely following participation?”. This question attempts to verify anecdotal concerns that participation may increase the overall risk of participation. This question ties to the research questions, and a positive would flag the participant of further interviews if possible. The final question was, “Would you be willing to participate in an interview?”.

The researcher received approval from the IRB on the survey questionnaire. The researcher sent the IRB-stamped consent form by email to potential responses. The researcher used personal cybersecurity connections to send the survey requests out. A single post on LinkedIn asked any additional responders interested to contact the researcher via the university

email address. The researcher sent out 75 survey questionnaires, and 39 respondents submitted responses. The researcher removed the responders and related agency/company names and put them on an indexed list to preserve anonymity as part of the research plan.

Interviews

The researcher conducted interviews in two locations in Aiken, South Carolina; the first location was a rented office in downtown Aiken and the other from the researcher's home office. The researcher used the home office for virtual interviews and the downtown location (providing convenience and easy access) for those willing to meet in person. Both sites provided sufficient privacy, comfort, and freedom from interruption to conduct the desired interviews.

Participants

Participant selection was a down selection of participants from tabletop exercises. The down-selection consisted of selecting the participant that meets the investigative needs of the study as determined by their survey responses. The study recognizes that most requested participants may not participate, so the goal was the utilization as many as possible. The researcher used the snowball method of gathering participants and use the linkages from initial contacts to identify more. The researcher compiled an initial network of cyber security representatives from across the country from which initial inquiries began. Local representatives reached out to their colleagues nationwide to aid in research. Local participants include city IT managers and emergency response planners (Aiken, South Carolina, Savannah, Georgia, and Augusta, Georgia). At the state level, participants include contacts from state law enforcement, larger businesses, universities, state-level emergency responders, and several representatives from the state school systems. Nationally, the more significant companies weighed in including computer manufacturers, software developers, and Army Cyber Command. The research

included those that had events that participated and did not participate in exercises.

Study Participants

The researcher randomly selected study participants by pulling from the community from recent cyber tabletop exercises using the broad spectrum of participants described previously. Participants were chosen based on the bins discussed earlier. Participants from municipalities, small businesses, and prominent government participants represent most of the target population. Based on the literature review, the expectation was that valuable information would likely come from the smaller business and rural municipality participants. The smaller partners carry the more significant portion of risk and are not as well represented. State and federal-level partners will provide a baseline for information and a possible hold-out data set for related questions or research validation.

The researcher asked participants to respond to demographic questionnaires about themselves and the institutions they represented. Additionally, the researcher allowed participants to answer questions based on their roles and expertise. The researcher recorded participants serving as subject matter or professional experts. Several candidates were initially identified in pre-work as this being a potential.

The initial goal of the data collection was to include a target of 30 participants. The initial sweep was posted on Linkedin and sent through ASIS, SLED, FBI, Army Cyber Command, NSA, and Air Force cyber networks led to initial candidate identification.

Sample Size

The research used pseudonyms and coded agency or company names to protect individual participants' identities. The number of participants originally targeted to include 30 participants in survey responses. The researcher surpassed the goal of 30, with 39 total

responders. The researcher reached saturation with four in-person interviews. Saturation was determined and proven through the continued replication of stories from each interviewee; as examples, all four retold stories where a smaller internet service provider was excluded from participation in a tabletop exercise and ended up being vulnerable, leading to a breach. All interviewees shared similar concerns over the same agency driving exercises that only address those agencies' concerns. Using similar language, all four expressed concerns that there was a small amount of deception in the overall risk reduction for participants. Additionally, saturation also showed that the issues extended across the United States and were identical. Not only where the participants aware of the issues related to missing participants, but they each cited multiple examples across the country. All four shared the same examples of issues in Texas, South Carolina, and Georgia. In the final saturation example, all four interviewees shared similar concerns in the open-ended dialogue. All four shared identical concerns about critical infrastructure information transmitted in an uncontrolled manner. All four interviews identified procurement documents that publicized vulnerability concerns. The vulnerability concerns occurred in different Requests For Proposals, but three of the four identified the same Request For Proposal as an example of inappropriate information. The fourth identified the same concerns but identified a different city as an example.

Procedures

The researcher received Liberty University's Institutional Review Board (IRB) approval. The final draft survey and interview procedures received expert field review. Once the IRB consented, the researcher piloted the survey and interviews with a small sample outside the study to ensure clarity of questions and wording. The researcher sent a notice of interest to the preselected groups to identify potential candidates. The research considered those that responded

favorably and met the demographic information goals. The researcher then selected a cross-cutting subset of participants and sent the preplanned survey to the selected respondents. The researcher then used an automated random sample of the completed surveys for individual interviews.

The Researcher's Role

The goal was to gather the information without influencing the provided data. The researcher limited the discussion topic to those outside the proposed pool. He has a pre-existing relationship with many of the participants, which will improve the likelihood of receiving responses. The researcher's relationship has been entirely tangential to the topic of research. The researcher participated in similar exercises in similar roles as those interviewed. As someone tangentially in a similar role, my concern grew to be of the questions not being answered or considered relative to tabletop exercises. The researcher’s previous position did not influence the outcome of the questions or responses as it was unrelated to previous experiences. The researcher balanced the questions so they did not lead to or direct a particular reaction. In addition to outside participants, the research included participants from within my former company. Although they were within the same company, they do not have a reporting relationship with the researcher during co-employment. Although the employees are in the same company, they were in different divisions, supported other clients. The benefit of utilizing these resources was that their roles in previous tabletop exercises are known. They were unaware of this research, were independent, and provided valuable insight.

The Researcher

The researcher worked in engineering and project management for 22 years and held a Bachelor of Science degree in Chemical Engineering and a Master of Science Degree in

Engineering. The researcher served as an active member of the Senior Executive Service for the Department of Energy in career reserved appointment from December 2022 until September 2023 and then transitioned back into a commercial role. The researcher had no relationship with any of the participants, so a conflict of relationship did not arise. The researcher and outside council evaluated whether the conflicts existed with the Department of Justice and Office of Personnel Management, Ethics Office.

The researcher has been involved in cybersecurity measures for the past five years, including serving as the South Carolina Law Enforcement Division's Nuclear Sector Chief as a Cyber Officer and the FBI Infragard's, National Security Sector Resiliency Program Chemical Sector Chief. The researcher stepped down from both agencies to complete this research without bias. The researcher has participated as an observer in previous tabletop exercises. Additionally, the researcher has participated in drills and training activities for nuclear emergency responses used as prototypes for cyber tabletop exercises. The researcher has conducted interviews and investigations with five years of experience as a law enforcement officer and three federal whistleblower-type investigations. Furthermore, he has ten years of research credibility established through formal audits by the Office of the Inspector General, Justice Department, and United States Senate.

Data Collection

The researcher collected data through field notes, interviews, surveys, and memos. Researcher field notes are a critical aspect of a qualitative inquiry with rigorous and varied data collection techniques. The researcher included data collection techniques in this section. (e.g., Erlandson, Harris, Skipper, & Allen, 1993; Lincoln & Guba, 1985; Merriam, 1988; Miles & Huberman, 1994; Patton, 1980, 1990). As an observer, the researcher attended several agency-

level tabletop exercises planned for 2022 and 2023. The researcher recorded observations directly in field notes. Surveys queried the larger population for the identification of participants and provided a larger community perspective. Data came from research memos, which provided formal documentation of agendas and goals of sponsoring organizations. Documented memos provided additional details on tabletop exercises.

Interviews

This research utilized a survey followed by an interview method where the interviewer asked open-ended questions. The researcher used field notes to document the responses to the questions. The initial questions were related to experience, exposure, and perceptions of tabletop exercises. The interviewee asked open-ended questions to identify motivation, correlation, and linkages between good events and training exercises. Interviews were conducted in person, electronically via teams, or over the phone. No discussion was conducted without the consent of the interviewee. The interviewees signed a digital consent form agreeing to participate in the study.

Standardized Open-Ended Interview Questions

1. Please introduce yourself to me as if we had just met one another.
2. Please walk me through your background in cybersecurity or tabletop exercises.
3. Describe your role and background in cybersecurity.
4. How does your division fit into the bigger picture of critical infrastructure?
5. What are your recent training exercises?
6. Have you or your division experienced a cyber attack?
7. Has any of the support infrastructure up or downstream been affected by cyber incidents?
8. Have you declined a tabletop exercise or another training event? Why?

9. Have the tabletop exercises you participated in been helpful?
10. Who was the sponsoring agency, and what do you know about their overall purpose?
11. How well were you prepared for your role in the tabletop exercise? Were you able to add value?
12. Was there another participant (or participants) struggling to fulfill their role?
13. What questions or value were you able to add?
14. As a group, where were there questions or sections left out? Did a fill-in play a sector's role during the scenario?
15. Did any groups disagree over a response due to similar scope or roles?
16. Following the tabletop exercise, were any changes made to your organization?
17. Have you had any cyber incidents since the exercise? Did the exercise help in any way?
18. This next question is unique in that it will invite you to look ahead. How will your organization participate in the future? Is there another alternative?
19. We've covered a lot of ground in our conversation, and I appreciate your time. One final question: What else would be vital about tabletop exercises?

Questions one through ten are knowledge questions (Patton, 2015) and follow-up to the survey questions. These questions are intended to be relatively straightforward and non-threatening and will build rapport (Patton, 2015).

The eleventh question asks the interviewee to self-reflect and may require vulnerability. This question arrives at a point where the interviewee and interviewer will have developed rapport (Patton, 2015). The twelfth question asks the same question but about others. Individuals are more likely to identify weaknesses in others, even if not in themselves.

Questions 13 through 15 examine the role-playing contexts in the specific tabletop exercises (Creswell, 2013). Question 14 may be vital in identifying the excluded participants. Question 15 seeks to identify duplicate role members. Questions 16 and 17 examine the effectiveness of the exercise by looking for changes completed after a training event. Question 18 looks to see what the organization plans to do going forward. The forward-looking question is essential to understand next-step plans in the context of both good and bad experiences. Question number 19 is a one-shot question (Patton, 2015) designed to give the participant another opportunity to offer valuable insight. The one-shot question acts as the closing question (Patton, 2015).

Observations

The researcher limited observations to the three tabletop exercises during the data collection phase of the allowed research. The researcher collected behavioral observations in addition to verbal transcription during the interviews. The interviewer observation protocol included descriptive and reflective field notes. The researcher acted as a non-participant observer during the tabletop exercises and an active participant in the interviews. The researcher collected the observations' frequency and duration; all were unscheduled.

Document Analysis and Artifact Analysis

The researcher reviewed historical reference document analysis and notes from previous tabletop exercises. Records evaluated included those not included in the literature analysis. Documents include CISA alerts, training documents, records, meeting minutes, letters, diaries, etc.

Observations

The data integrity and credibility of the research was paramount. A data transparency approach ensured comparability, scrutiny, audit, or any other question that may arise. The researcher recorded and transcribed every interview. The archive was made available, and data analysis used standard approaches traceable back to the original data set. Furthermore, the researcher used an independent auditor to review the findings before submission back to the committee chair.

Memos

The document formality of memos added to the integrity and credibility of the research. Formal research memos provided documentation of agendas and goals of sponsoring organizations. This verified information provided a basis to test for impacts on the outcomes of the tabletop exercises. The observations from professional or educational institutions provided additional details on tabletop exercises.

Data Analysis

Open, axial, and selective coding are appropriate for grounded theory studies. Each data set and then synthesize findings across all three (or more) data sets. Some forms of coding, bracketing, and memoing are tools commonly used to organize data and identify recurring themes for many qualitative data analysis strategies. Independent traceability ensured the data was valid and accurate.

Trustworthiness

Using established means, methods, and process transparency improved the trustworthiness of the research. The researcher has recorded the responses in their original format

digitally hardcopy, and both are available for review upon request. The researcher considered the degree of confidence in data, interpretation, and methods used to ensure the quality of a study (Connelly, 2016). The researcher established the protocols and procedures necessary for a survey to be considered worthy of consideration by readers long before beginning any research.

Credibility

Credibility refers to the extent to which the findings accurately describe reality. Credibility depends on the richness of the information gathered and on the analytical abilities of the researcher. The research questions were framed in multiple ways so that there was no leading to an answer to minimize bias.

Dependability

The researcher addressed the dependability of the research by utilizing proven methods, including direct transcription of interviews, member checks, prolonged engagement, and documentation validation where possible. Direct transcription reduces common errors in qualitative studies (Easton, 2000).

Transferability

Transferability refers to the possibility the results of this study will translate into other contexts. The findings of this research will directly cross-walk to tabletop exercises sponsored in different contexts, such as the medical field or emergency response outside of cyber.

Dependability and Confirmability

The researcher addressed the dependability and confirmability through every step of the study. An independent audit of the analysis provided overall veracity. Through a comprehensive analysis of the participants, the companies involved, in-depth interviews, and independent

confirmability of the results, the researcher adequately addressed dependability and confirmability.

Ethical Considerations

Participants signed consent forms electronically before the survey started. The researcher reviewed the informed consent verbally before any of the open-ended interviews. The informed consent followed the required guidelines and ensured the participants knew they could stop at any time (Frankfort-Nachmias, 2008). The study itself presented only minimal risks to the human participants. The researcher addressed data storage and usage, influence, confidentiality, and other potential issues by air-gapping all information. The researcher only presented summary information within the attached appendices.

Summary

The implications of not having appropriate representation from all integrated partners involved in a tabletop exercise, the act of participating, and the level of involvement affect the exercise's efficacy. The research methods will investigate who participated in recent tabletop exercises. In this section, the researcher reviewed the study's impact and the results' risk, credibility, and reliability. A survey screened participants before one-on-one interviews. The researcher determined that grounded research was the most appropriate form of investigation.

CHAPTER FOUR: FINDINGS

Overview

This qualitative study evaluated the impacts of participating in tabletop exercises to prevent or mitigate cybersecurity events. The tabletop exercise is the single way of preparing for multi-source and multi-vector cyberattacks in which the entire community responds.

The research was conducted in three phases. Phase One focused on a survey sent to the general emergency preparedness or cybersecurity community of practice. Phase one elicited information through questions geared to set macro-level broad perspectives on the tabletop experience, the value of training, and, most notably, to identify a subset of participants for phase Two. Within phase one, the research covered the value to the participants. These were also compared with attribute information from respondents to capture a baseline for further exploration in later phases.

The research focused on open-ended interviews with selected participants in Phase Two. In this section, the researcher provided a rich background of the interviewees and details about their experiences. The interviewees shared experiences and faults that came with actual events, and those in training repeatedly shared the same information. The researcher hosted the first three interviews in Aiken, SC. The fourth was scheduled and conducted virtually. The primary investigator met with the first two in the open office space reserved for this study. The second participant was interviewed twice, both in Aiken, SC. The final two interviews were completed virtually over Microsoft Teams.

In Phase Three, the investigator observed tabletop exercises in person while taking notes. Based on the research window between IRB approval and the completion deadline, the researcher expected only a limited opportunity to view in-person training. Phase three included

two direct observation opportunities to conduct longitudinal interviews with one participant (interviewee two) who participated in three separate tabletop exercises. United States Government agencies sponsored the actual observations of two tabletop exercises. The participants included a full spectrum of support agencies, private industry, and no unique or out-of-ordinary methods.

The organization of this chapter includes an evaluation of survey respondents and a summary of their responses, as well as their perspectives on the individual survey questions. The survey also established a baseline for respondents and participants in these training events.

Participants

The survey responses included 39 participants. The breakdown of company and size yielded larger companies than smaller ones. The participants selected for further interviews included additional information in their survey responses indicating participation in multiple tabletop events. Although this was unsolicited, the additional information made them valuable targets for data collection. Participation and subject matter expertise were significant to ensure that the research was credible.

The investigator offers the following pictograms of the individuals interviewed. The researcher removed the company and agency names to protect their identity. This research excludes their names and genders randomly changed to protect their identity. The researcher tried to obscure their real identity, except for their life experiences. Their pictorial descriptions are accurate and as relayed. Converting genders was required to ensure anonymity based on life experiences (random).

Interview One

Interviewee one represented a unique set of interviews. Interviewee one is a long-term United States government employee with a large federal agency (cabinet level). He is a supervisory GS-15 employee deployed in a field office away from Washington, DC. He has more than 30 years of experience. During that time, he spent 15 years in the day-to-day operations of a high-hazard facility. The role of the facility was packaging and handling of hazardous material. The facility was also highly regulated. In that role, he interfaced regularly with state environmental regulators and federal law enforcement. Following that assignment, he spent four years in another division of the same agency developing long-range strategic planning initiatives. He has been a director for the last 16 years, supervising a team of 10-20 employees. He manages the projects with a yearly operational $500 million budget. He oversees many smaller non-capital projects and interfaces with the public and government agencies. He is married, has two grown adult children, and is only a few years away from retiring. Interviewee one provided a government agency perspective in participating in tabletop exercises.

Interviewee one does not have a background in cybersecurity but is a subject matter expert on emergency response. He holds a degree in Mechanical Engineering but has not engaged in technical work for the last 15 years beyond program management. He does own an Emergency Response Operator qualification from a government agency. Obtaining and maintaining that certification has required National Incident Management Response training annually from the Department of Homeland Security (DHS). The DHS training required courses NIMS 101, 200, and 401 and site-specific emergency response training. On average, he has participated in emergency response tabletop drills once a quarter for the last 15 years.

Interviewee one participated in tabletop exercises as a stakeholder, agency representative, and government oversight of contractor exercises. He most routinely represents his agency as the senior spokesperson/decision-maker for the government. In his exercises, his set of facilities has regularly scheduled tabletop events across various incidents, including national disasters, terrorism, insider threats, and even industrial accidents. Interviewee one participates in a once-a-year cyber-only attack exercise. He participates in several other tabletop exercises that are emergency response or security-related.

His initial interview provided generally expected information from his past experiences with tabletop exercises. He was critical of his involvement in tabletop exercises. He did not believe he added value but saw the importance of exercise. Interviewee one had two more drills scheduled after the first interview. Interviewee one provided a longitudinal view of how tabletop exercises have changed. The researcher asked if he could follow up with the participant after each exercise to get his feedback, and Interviewee one agreed. The three interviews all occurred in Aiken, and the feedback and perceptions of all three were different. Although his experiences differed, they were congruent with the other interviewees and contributed to saturation.

Interviewee Two

Interviewee two has 16 years of experience as a commercial cybersecurity expert. He is a regional representative for his company, company one. Company one has 200 employees and an annual revenue of $50M. He has worked in many cybersecurity roles, from Analyst, IT Manager, Cyber Security Engineer, Cyber Security Program Manager, and current regional Cybersecurity Director. He has a BS and MS in computer science and numerous certifications, including Certified Information System Security Professional CISSP, Information System Security

Engineering Professional (CISSP ISSEP), and Certified Ethical Hacker. Interviewee two is a mid-career professional from a commercial business.

His involvement and interactions are different from the interviewee ones. Interviewee two interactions have taken various roles. In reality and tabletop exercises, he has served as a cybersecurity first responder and is a security provider. In several training events, he would watch the testing of his security products. Interviewee two provides contract security in the case of an event. These are active response contracts, recovery contracts, and even active mitigation. Most of his work is in preparing and pre-planning to prevent an attack.

Interviewee two has a younger family and aspirations of someday starting his own business. His perspective on cybersecurity is that it is the most serious issue facing the United States. His breadth of experience covers prevention and response during an active attack.

Interviewee Three

Interviewee three works at company two and has 25 years of experience. Interviewee three has a background in physical and cybersecurity. Company two is a substantial commercial company. They employ 44,000 employees worldwide and $9 billion in revenue. Interviewee three's company division provides technical support primarily to government agencies across the globe. Interviewee three's prior experience provided physical security to nuclear facilities. This experience included research, power production, and environmental restoration projects. Interviewee three has no technical degree but has risen to a senior role based on his experience and capabilities. In addition to his commercial work, he is also an active member of Infragard. The Infragard is a collaborative effort between private and industry and the Federal Bureau of Investigation (Infragard 2019). Infragard members are vetted and bidirectional to share information with various US Governmental agencies (Infragard 2019).

Interviewee three serves as a subject matter expert for profit to other commercial firms and the government. His clients have included small municipalities, states, and nearly every critical industrial sector. He often serves as a consultant, improving corporate policies, procedures, training, and cyber programs. He has conducted penetration testing but has written many policy and procedure changes. He has over ten years of experience participating in tabletop exercises related to cybersecurity events.

Interviewee Four

Interviewee four is a Subject Matter Expert in Software Architecture. He is actively involved in cybersecurity applications. Cybersecurity considerations are a daily part of his job, but he is not engaged in threat hunting, cyber protection, or similar activities. Interviewee three spends most of his time writing code or developing software requirement documents for simple process automation. He is in a regulated industry, and cybersecurity is a crucial aspect. Interviewee four works for a small company with many high-profile customers.

Interviewee four described the importance of understanding the cybersecurity requirements of software development and installation; ensuring that his business and the agencies he supported complied was one of his most important priorities. He has minimal active experience with actual cyberattacks but extensive experience in the prevention portion of cyberattacks.

Interviewee four participated in six tabletop exercises related to cyberattacks. Those experiences cover two sponsored by state-level agencies and four from a federal perspective. Interviewee four has also worked with a wide range of customers. His customers include large companies, agencies, and local municipalities. The experience working with municipalities may provide additional customer insight into smaller markets and their unique challenges.

Credibility of Participants

An essential aspect of the interview participants was their ability to speak at a more educated level for the cybersecurity community. Based on the potential of one or two participants to sway the study, participants who met the inclusion criteria were selected. Important factors included education, certifications, experience, and emergency response/security experience. The four interviewees each represented a different business sector, from small to large, and even the federal government. An additional area of concern was the various aspects or roles each could play in a team. Having the entire interview list consist of individuals of the same role and responsibilities encouraged response diversity. The response diversity did not impact the ability to reach saturation. Despite the efforts to promote as varied responses as possible, all interviewees returned similar or identical responses. The response similarity further established the research's credibility. The researcher's second consideration was the interviewee's role in cybersecurity. The role of cybersecurity and the corresponding position in the tabletop exercises could have potentially provided different perspectives. The researcher intended to span more than just the size of the business, but the various roles within a tabletop exercise were critical in proving credibility with the results. The varying business sizes returned the same results, and the roles made no difference. Saturation occurred even with varying multiple factors.

1. Interviewee One –Federal Government, Sr. Government Technical Authority
2. Interviewee Two – Medium Commercial Business, Cyber Threat Analyst
3. Interviewee Three – Large Commercial Business, Cybersecurity Policy
4. Interviewee Four – Small Commercial Business, Software Development

All four interviewees have the potential to affect the outcome of the study. Nothing was more important than finding the right team of individuals to question. Each of the experts chosen had a role within the cybersecurity envelope. They all had experience participating in tabletop exercises, and each provided a perspective unique to their experience. The researcher ensured he did not lead the interview. The responses were solely those of the respondents.

Results

The results of the research were organized into three phases. Phase One focused on electronic questionnaires or surveys. The survey respondents included 39 completed questionnaires. Phase Two focused on individual interviews with four subject matter experts. Phase Three included the direct observation of two cybersecurity tabletop exercises; the original questionnaire provided some interesting insights that were unexpected during the initial development. The investigator asked 19 specific questions during the interviews. The researcher did not always ask them in order. The researcher also encouraged the interviewees to share anything related to the questions they felt was relevant. Following the interviews, the researcher reviewed the interview notes for themes. The researchers developed themes around the original research questions. Several other foci outside of the actual research questions became apparent. The researcher analyzed the responses based on theme, language, and context. The investigator compared the research questions and focus of this research. The theme development uses specific quotes from the interviews with the appropriate narrative to provide context. Quotes are as stated except for a few instances in which they disclosed personal names, personal information, and business or agency names. The researcher moved the locations of incidents to a higher level to limit the ability to reconstruct the interviewees' identities. Although beyond the scope of this

research and research questions, much of the data collected could have uses outside of this research.

Theme Development

The researcher considered and developed numerous themes based on the analysis models identified. In addition to the various themes, the researcher evaluated the grouping and relation of responses to each other. The most apparent sorts of data were around the original research questions. The researcher also considered the negative and positive responses. The researcher grouped the positive and negative responses, seeing if additional themes emerged. Response analysis included tone, verb, and negative/positive responses. Varying the positive and negative during questioning also elicited fuller responses. To remove question bias, the researcher took all of the available data and attempted to consider it from as many perspectives as possible. The researcher reviewed the interview data and binned all negative versus positive content.

The researcher collected the primary information for thematic development during the interviews. The researcher used surveys to query the larger population for the identification of participants and to provide a more extensive community perspective. The results of the researcher's final interviews were comprehensive surveys and memos and research notes taken on the actual observations of the two tabletop exercises (Erlandson et al., 1993; Lincoln & Guba, 1985; Merriam, 1988; Miles & Huberman, 1994; Patton, 1980, 1990). The researcher sought and collected memos that provided formal documentation of agendas and goals of sponsoring organizations in the tabletop exercises. The memos provided a clear expectation of goals and alignment for the sponsoring agencies so that the researcher could compare the intent and agenda to the impact in the field.

The most significant themes from the data questions were related to the original research questions. Using a negative or positive approach provided additional insight. The opposing themes included non-compliance, missing participants, lack of training, budget, staffing, and awareness. The researcher observed several new issues not identified initially. The emergent issues included non-compliance and issues related to the tabletop exercise's historical legacy.

Noncompliance

Interviewee one stated, "Noncompliance was the number one problem affecting his agency and their role in all tabletop exercises." Not only was his agency non-compliant, but leaving the meetings, exercises, etc. "there was insufficient time or budget to implement what they knew they should already be doing, much less doing something more." Identifying new issues or risks would not help because they had yet addressed current known issues.

Organizational noncompliance is when an organization fails to adhere to laws, regulations, industry standards, contractual agreements, or internal policies and procedures. Noncompliance can occur in various areas, including legal, ethical, financial, environmental, cybersecurity, and data privacy (Bulgurcu 2010). Sometimes, noncompliance occurs due to a lack of awareness or understanding of relevant laws and regulations; however, cyber non-compliance seems more driven by cost. Interviewees two, three, and four added to this concern by citing numerous examples where teams new they had non-compliance issues but chose not to implement solutions. Furthermore, they demonstrated saturation by singling out several agencies worse than others in organizational non-compliance. Each interviewee also named the same agencies entirely independent of each other, although they all had different roles and backgrounds.

Another exciting discovery during the interviews (interviewees one and three) was that the Design Basis Threat drove most of the responses for security in the government. The Design Basis Threat (DBT) is essential in infrastructure protection and facility security planning. A DBT is a comprehensive and systematic description of potential threats and risks that an organization, facility, or system the security professional uses to define the hostile threat. The DBT is a foundation for developing security measures and procedures to protect against these threats. Interviewee three stated, "A non-realistic DBT leaves the facility vulnerable to the next attack but makes the government feel better." The DBT outlines potential threat actors or groups that could pose a security risk. These could include terrorists, criminal organizations, activists, insiders, or other malicious entities. More critical than identifying the who, interviewee three asserted that "the DBT identifies their capabilities and what they are capable of doing." The DBT assesses the capabilities and intentions of threat actors. It considers factors such as their access to resources, expertise level, and motivations. The DBT gets tested through tabletop exercises and vulnerability assessments to ensure they are effective. "The DBT sets the tabletop exercise for failure if you show up with neutered terrorists," interviewee three. What makes this more challenging to address is that the "DBT is often classified or worse treated as sensitive" and not reviewable, according to interviewee three. The reason for the control of the information is to prevent the release of security-related information. Interviewee two added to this discussion by stating they were "not required to protect their operations from threats greater than their design requirements." He said, "The design requirements no longer cover the real threat."

Tabletop Mentality and Process Baggage

Along with the same negative information received, two of the four interviewees (two and four) stated that the nature of tabletop exercises fails to meet cybersecurity needs. When

probed further, interviewee two said, “The potential that the setup in general is problematic.” He explained that “using an emergency response method to deal with a day-to-day hazard is ineffective.” Interviewee four added to this concept when he stated, "Tabletop exercises are very effective, but they come with baggage. All of the emergency response meet once a year, and concepts flow into these exercises.” Tabletop exercises are used routinely for hazards and emergency response. In other industries, these issues are rare. Cybersecurity events are happening every day, and utilizing a tool used currently for rare events is problematic.

Impact of Cascading Events on Cybersecurity

Cascading events can profoundly impact cybersecurity by exacerbating vulnerabilities, increasing the complexity of security incidents, and potentially leading to more significant and widespread breaches. Cascading events in cybersecurity occur when one security incident or breach triggers a chain reaction of additional incidents or vulnerabilities. As evaluated in Chapter one, the impact of cascading events was of potential concern. The interviewees were concerned about cascading events and the relationship to attack vectors. Interviewee four spent significant time after the standard questions discussing how he could do everything right. However, he has countless unknown vulnerabilities based on how others could impact his system. Interviewee four stated that “every web application, data transmission, and even the internal components of my computers represent vulnerabilities for which I have no protection. Cybersecurity tabletop events are the only time we discuss mutual trust and risk.” The procedures and laws are consistent from one group to another; however, the various organization's implementation can vary.

Interviewee three provided an example: "A successful phishing attack on one employee's account can lead to unauthorized access to sensitive data and serve as a launching point for

further attacks within the organization. However, it does not stop there. An initial breach allows attackers to move laterally through the network, gaining access to more critical systems and data. Eventually upstream and downstream to everyone else we touch." This escalation can lead to more extensive data loss, financial losses, and reputational damage.

Standardized Open Ended Research Question Responses

The researcher conducted the interviews according to the procedures in Chapter Three, with the participants identified in Chapter Four. An original list of questions and summarized responses are in this section. Questions one through five establish the background information included earlier on the four interviewees.

Question 6 asked, have you or your division experienced a cyber-attack? All four of the responders have experienced cyberattacks beyond the tabletop exercise. Interviewee one provided less detail than the other three. Interviewee two and interviewee three corroborated several specific accounts of cyber-attacks related to multiple agencies at all levels. They both provided details on cyberattacks following tabletop exercises.

The interviewees shared the same story independently of an internet service provider being attached days following a tabletop exercise. The agencies breached were a Tier One Executive Law Enforcement Agency and a state-level law enforcement agency. Interviewee two stated, "One day after a tabletop exercise, they noticed unusual network activity. Within twenty-four hours, [Another Agency] notified them that a large portion of their data was available on the dark web." Interviewee three retold the same story but added that the data available "was related to the home addresses and phone numbers of all the law enforcement officers' personal information." They both corroborated that the exact source of the breach was the internet service provider for the state agency. Interviewee two stated that "the internet service provider did not

attend and did not participate in the tabletop exercise. Interviewee three added that if "the internet service provider had been considered part of the network, they could have prevented the breach." The response to this question also answered question seven.

All four interviewees knew of downstream and upstream attacks that affected cybersecurity. Two interviewees added that distributed dependence on each other caused a need for a zero-trust approach or paradigm shift in security to keep improving security.

The researcher asked several questions to understand the preparedness and selection for participation in the tabletop exercise. The more significant question that was unclear was who should come, what career level they should be, and whether their training would be helpful. Question nine asked, have the tabletop exercises you participated in been beneficial? In the first discussion with interviewee one, he stated, "I was the wrong person to be there, but the experience was positive." The researcher questioned interviewee one more than once. He had three different experiences. He also had lots of experience in participating in these types of exercises. In his first experience, he stated, "he did not feel adequately prepared for the exercise." In the second exercise, a federal facility representative briefed on the status of the facility work inside and operations underway. "The facility representative gave me details on potential drill scenarios and what security professionals need to do. I was much more prepared," stated interviewee one. Following the second drill, interviewee one reported being well prepared and the exercise being more successful. In the third scenario, an extra observation was allowed, and the results were "I added value, and I am glad I was there." For all practical purposes, all three exercises were identical. The only difference between them was a briefing in the second. His experiences illustrate that a brief preparation before the exercise may be of more value than training, experience, or scope. The takeaway is that a focused preparation for a tabletop exercise

may be more helpful. The needed preparation may not always be possible but would mirror the transition of command requirements as outlined in NIMS training (DHS, 2008). The responses to the remaining questions were summarized directly related to the Research Questions.

Themes Around Research Questions

The Research Questions aided theme development. The research questions are below:

- **RQ1**: What is the impact of having the wrong or missing participants in a tabletop exercise?
- **RQ2**: What is the consequence of participating in a tabletop exercise? Does this cause additional risk?
- **RQ3**: Do the agenda, goals, and objectives impact the outcome of the tabletop exercise's effectiveness?

The survey and research questions show an interconnection between them in the table in Appendix A and the interrelationship between Primary and Secondary connections with the research questions.

Research Question 1

RQ1: What is the impact of having the wrong or missing participants in a tabletop exercise?

The result of not having the right participants is that the exercise uses stand-ins that do not know how the actual agency will respond. Interviewee one, interviewee three, and interviewee four all provided detailed examples of how an actor or stand-in offered non-sensical solutions to what the actual agency or group would have done. Having a missing organization or participant causes complications in response and leads to unrealistic responses. Three cases cited by the interviews demonstrated the risk of not having the right participants. The data shows that better efforts could have prevented attacks. Interviewee one interrelated two research questions,

one and four, with his response. He saw “no risk from having missing participants as long as his agency met its needs.”

Combining the themes analysis and recentering under research questions from the data during the interview analysis identified numerous consequences to research question one.

- Missing participants hurt the overall exercise. Stand-ins or actors do not provide the same level of insight that the correct participant would have.
    - Incomplete Assessment: Missing key participants can lead to a preliminary assessment of the organization's response capabilities. For example, interviewee three responded that if “critical decision-makers or subject matter experts are absent, it may be challenging to evaluate the effectiveness of decision-making processes or the technical response to specific scenarios.”
- Missing or wrong participants cause additional security gaps for those participating. As previously discussed, leaving out one party led to significant security breaches in prestigious agencies.
- Missing participants hurts those who do not participate.
- Incorrect participants (wrong level or expertise) are only slightly better than not participating at all. All four interviewees expressed this opinion.
- No conclusions were reached on what career level, experience, years of service, or training could be definitively quantified on who should participate. The researcher observed that this question's response was person-dependent.

Several subthemes also developed underneath Research Question 1. The researcher captured missed opportunities and unrealistic biases or assumptions.

Missed Opportunities for Improvement: Tabletop exercises are valuable for identifying weaknesses and areas for improvement in an organization's response plans and procedures. The wrong or missing participants can lead to missed opportunities to identify and address these weaknesses.

Unrealistic Assumptions: The absence of critical participants may lead to unrealistic assumptions about their actions or contributions during a crisis. Unrealistic assumptions can result in overestimating or underestimating the organization's response capabilities. Careful planning maximizes the value of tabletop exercises and necessitates the coordination of participants and their roles. The appropriate participants include representatives from various departments, decision-makers, technical experts, and anyone who would play a significant role in a real crisis.

Research Question 2

RQ2: What is the consequence of participating in a tabletop exercise? Does this cause additional risk?

The responses on benefits of participation include multiple significant consequences, all intended to improve preparedness and response to various scenarios. The primary consequences of participating in a tabletop exercise include:

Enhanced Preparedness. Tabletop exercises simulate real-world situations, allowing participants to practice and refine their response strategies. Real-world practice enhances preparedness by helping individuals and organizations become familiar with their roles and responsibilities during a crisis.

Identification of Weaknesses. Tabletop exercises often reveal weaknesses in an organization's plans, procedures, and processes. Weaknesses can include gaps in communication,

inadequate resources, unclear decision-making hierarchies, or overlooked vulnerabilities. Identifying these weaknesses is a crucial step in improving overall readiness.

Learning and Skill Development. Tabletop exercises give Participants valuable experience and knowledge. They learn to handle various scenarios, make informed decisions under pressure, and work effectively as a team. The security professional can apply these skills during actual emergencies.

Improved Communication. Effective communication is a cornerstone of crisis management. Tabletop exercises help participants practice communication and coordination within and between teams or departments. Improving communication can lead to more efficient and coherent responses during actual crises.

Risk Mitigation. Organizations can proactively mitigate risks and strengthen their security posture by identifying weaknesses and vulnerabilities through tabletop exercises. Mitigating risks can include implementing new security measures, updating response plans, and enhancing employee training.

Stakeholder Collaboration. Tabletop exercises involve internal teams, external partners, and relevant authorities. Collaborating in a simulated crisis environment fosters relationships and understanding among these stakeholders, which can be invaluable during a real crisis.

Participating in a tabletop exercise is a proactive and valuable endeavor that helps individuals and organizations prepare for and respond to crises more effectively. The consequences of these exercises are generally positive, leading to improved readiness, better coordination, and a more robust response capability when faced with real-world emergencies.

The second part of research question 2 focuses on the additional risk posed by participation. Participating in cybersecurity activities can carry other risks for individuals and

organizations involved. These risks can vary depending on the specific nature of the activities, the roles and responsibilities of those involved, and the geopolitical context. One of the critical factors is the amount of information control related to participation.

Physical Risk / Physical Identification. Individuals engaged in counterterrorism activities, such as law enforcement officers, military personnel, intelligence operatives, or security contractors, may be publicly identified following participation in a tabletop exercise. The results or findings may be published, leading to the identification of people, places, and vulnerabilities. Unintended disclosure creates the risk of confrontations with terrorists, combat situations, or attacks aimed at utilizing identified vulnerabilities, attacking the weakest link, or disrupting cybersecurity efforts. All of the interviewees identified this as an issue. Each has specific examples of organizers or planners publicly releasing information in after-action reports.

Loss of Anonymity. Counterterrorism, cybersecurity, emergency, and even law enforcement professionals may lose their anonymity, making them more vulnerable to threats and targeting by terrorists who seek to identify and retaliate against those responsible for thwarting their activities. The most impactful stories were of state and municipal agencies that participated in good faith and had some critical vulnerabilities attacked following events. A generalized lack of concern existed from agency tier to agency tier.

Research Question 3

RQ3: Do the agenda, goals, and objectives impact the outcome of the tabletop exercise's effectiveness?

Interviewee one answered this question first with a resounding yes. Interviewee one stated, "Yes, the sponsoring agency's agenda, goals, and objectives can significantly impact the effectiveness and outcomes of a tabletop exercise." The agency drives the goal and funds the

exercise. The sponsoring agency dictates the design and focus of a tabletop exercise in alignment with the intent and what it seeks to achieve. Interviewee one was the only one who answered this question so firmly. The other three provided softer answers. Allowing the interviewees to expound on how the goals and objectives of the tabletop exercise impacted the event itself yielded consensus. Outside of the first interviewee having already thought through this issue, the other three also demonstrated the level at which saturation was met by repeating identical stories. All three retold events where the exercise was close to yielding practical information that would have been useful, but the event terminated early, or a discussion point was cut short due to an intervening sponsor. Interviewees two, three, and four shared that issues or discussion points often were “tabled” or “saved for later” at the direction of the event sponsor, once again reinforcing saturation.

The sponsoring agency determines the scenario for the tabletop exercise. The chosen scenario should align with the agency's goals and objectives. For example, suppose the agency's primary concern is a cyberattack on critical infrastructure. In that case, the exercise scenario will revolve around this, and the planner will test the effectiveness of the response to that specific threat. The interviewee was the first to raise the issue of the objectives of the exercise, cutting outside discussion short. Three interviewees described how the agency set the objectives and learning goals for the exercise. These objectives outline what they hope to achieve, such as testing specific response procedures, evaluating communication protocols, or identifying weaknesses in the organization's crisis management plan. The planners measure the exercise's effectiveness against how well it meets these objectives.

The sponsoring agency's agenda impacts the realism and relevance of the exercise. If the agency is primarily concerned about natural disasters, they may design an exercise simulating a

major earthquake or hurricane. The exercise may involve a simulated cyberattack if they focus on cyber threats. Realistic scenarios that reflect the agency's concerns are more likely to lead to valuable insights. All four interviewees note that the agency determines who participates in the exercise and which external stakeholders are involved. The interviewees also said they had seen some sponsors select who to invite and declined to include some participants. The choice of participants and stakeholders should align with the agency's objectives. For instance, if the agency aims to improve coordination with local law enforcement during a crisis, planners include representatives from law enforcement agencies.

The agency's goal influences the level of complexity and the scope of the exercise. An agency looking to test high-level strategic decision-making may design a more complex, organization-wide exercise. Alternatively, planners narrow the scope of a specific aspect, like communication, as the focus. Three interviewees expressed concerns that they had witnessed the sponsoring agency stop discussing issues unrelated to their objectives.

The sponsoring agency defines the criteria for evaluating the exercise's success. These criteria often relate directly to the agency's objectives. Interviewee three provided the example of the objective to assess the effectiveness of incident reporting; the evaluation focused entirely on how well participants reported and documented incidents. Interviewee three stated that the "exercise did nothing to protect those attending, only improved reporting." The agency's agenda also impacts what happens after the exercise. Depending on the goals, they may expect specific follow-up actions, such as revisions to response plans, updates to policies and procedures, or additional training. The effectiveness of the exercise is measured, in part, by how well it informs and drives these post-exercise activities.

The sponsoring agency must clearly understand its objectives and communicate them effectively to all participants and stakeholders to ensure the effectiveness of a tabletop exercise. This alignment between the agency's agenda and the exercise's design and execution is essential for achieving the desired outcomes and enhancing preparedness and response capabilities.
The exercise.

Summary

This qualitative study evaluated the impacts of participating in tabletop exercises to prevent or mitigate cybersecurity events. A tabletop exercise is the single way of preparing for multi-source and multi-vector cyberattacks in which the entire community responds. The organization of this chapter included an evaluation of data gathered from respondents. The survey responses included 39 participants out of more than 75 requested. The researcher interviewed four individuals: one from a small, medium, and extensive business and one federal employee. The interviewees all had various roles related to cybersecurity. Although there was overlap in each interviewee's background, they represented different perspectives and were familiar with the tabletop exercise to be considered experts. Saturation occurred relatively quickly during the interviews based on the interviewee’s responses. The interviewees repeated similar stories and themes and raised the same concerns. Although they had participated in many different exercises, they told story after story that repeated information already provided. The research interviews began to reach saturation by the second interviewee, and the final two interviews confirmed that no new or additional information, themes, or insights would come from other interviews. The interviews provided sufficient information to address the research questions effectively. The researcher confirmed saturation through the same themes, patterns,

and ideas repeatedly mentioned by participants. The final two interviews confirmed data redundancy.

As discussed, the researcher used several methods for theme development. The first focused on positive and negative responses to the interview questions. This approach yielded findings about noncompliance, tabletop baggage, and cascading events. The remaining themes were related to the three research questions: the impact of having the correct participants, the consequence of participation, and the impact of the sponsoring agency. Two additional themes were identified in research question one: the missed opportunity for improvement and the consequence of unrealistic assumptions.

CHAPTER FIVE: CONCLUSION

Introduction

This study aimed to evaluate the impact and use of tabletop exercises in preparation for cybersecurity defense in systemized attacks. This chapter reviews the conceptualized role of the tabletop exercise in cybersecurity preparedness and the key findings of the research. The six sections include an overview of the chapter, a summary of the findings, a discussion of the implications considering the relevant literature and theory, an implications section (methodological and practical), the study delimitations and limitations, and recommendations for future research.

Overview

Cybersecurity and security protection comes from many different means. The primary method for ensuring cybersecurity in dispersed attacks is through tabletop exercises. Most other forms of cybersecurity focus on the individual, the individual computer, the individual company, or an individual component. Tabletop exercises are a community event where various stakeholders look at realistic scenarios from an event to address the overall response. Criminals often prefer to use non-traditional attack vectors. The element of surprise increases the likelihood of success. The most accessible point of attack is an unprotected one. These exercises prepare for emergencies and terror attacks. The benefit of these training events is the opportunity to see how each participant, often representing various organizations, would respond to an attack and to identify vulnerabilities. However, there are concerns that these events often fail to include the right participants from both an individual responsibility level and an industry perspective. The sponsoring agencies may influence the exercise, and participating may even lead to a higher threat of subsequent attack.

The literature review provided a comprehensive review of relevant literature to demonstrate the current understanding of the existing research and how the proposed research questions fit into the broader academic context. The researcher evaluated the published information related to tabletop exercises related to cybersecurity. The Army Cyber Command has recently sponsored multiple agencies and commercial exercises to help prepare for future attacks through their Jack Voltaic series. The biggest takeaway from literature research is that these types of engagements are effective. Previous research also identified, from attack data, that criminals continue finding new ways to wreak havoc on public systems. Previous research also highlighted these types of community role-playing have been effective. There are also other numerous correlates between healthcare, emergency response (non-cyber related), and even terror attack planning that informed this research. This research may also be beneficial to those areas as well.

After conducting the initial research and observing several tabletop exercises, the researcher sought better answers to improve these interactions. Anecdotally, many individuals appeared to be attending, and many were not. Several events occurred immediately following significant tabletop exercises, and it was unclear how the tabletop improved security. The researcher simplified the critical research questions utilizing the literature review of all the information available to **RQ1**: What is the impact of having the wrong or missing participants in a tabletop exercise? **RQ2**: What is the consequence of participating in a tabletop exercise? Does this cause additional risk? **RQ3**: Do the agenda, goals, and objectives impact the outcome of the tabletop exercise's effectiveness? The researcher developed a strategy to address the initial research questions and another overarching issue. The most common theory applied in security is the weakest link model. The literature research suggested several other models that may be a

better fit to describe observed behavior. The researcher proposed that the fractured flaw may be a better fit.

The data harvesting approach included research methods, and data collection techniques grew through multiple phases. The first phase sent a questionnaire to industry experts about cyber tabletop exercises. Several of the questions also led to some overall conclusions and insights independently. From those questionnaires, the researcher selected individuals for Phase Two, individual follow-up interviews. The researcher achieved saturation after four interviews related to cybersecurity and tabletop exercises. These interviews reached the point of subject exhaustion and provided many insights. Although in different roles, companies, and varying perspectives saturation was confirmed through repetition of the same concerns. The interviewees repeated the same stories and the thematic responses provided confirmation on the research results. One set of interviews allowed the same participant to interview following multiple tabletop exercises. Phase three included field observations of two tabletop exercises and collected data relative to the research questions. The data analysis included in previous chapters presents the results of the research in a clear and organized manner. The data discussion and interpretation, as well as the findings' implications, achieved the research goals.

The goals of all three phases of data collection were to provide insight into the best techniques for team selection and best practices approach to improving post-training security. Understanding the risks, gaps, and other considerations is critical to improving responsiveness and security.

Summary of Findings

The primary findings answered the research questions; additionally, the advantages of the fractured flaw theory develop as an alternative to the weakest link. The results significantly

expanded on the current information and research available. The core findings were that missing participants was a significant detractor from table to exercises.

Research Question 1 Findings

The first research question focused on missing or wrong participants. Every planning event attended before this research officially started saw this question asked without any clear resolution. Interviews with participants led to some specific conclusions. Research question one was: What is the impact of having the wrong or missing participants in a tabletop exercise? The resounding response from the interview saturation was that not having the correct participants led to multiple issues. Having a missing organization or participant causes complications in response and leads to unrealistic responses. Three cases cited by the interviews demonstrated the risk of not having the right participants, explicitly leading to preventable attacks. One inter-related research question from respondent four showed that agency priorities drive improper participant selection. One respondent saw no risk of having missing participants as long as he met his agency's needs.

The results to research question one, what do missing participants do to an exercise?

- Missing participants hurt the overall exercise. Stand-ins or actors do not provide the same level of insight that the correct participant would have.
- Missing or wrong participants cause additional security gaps for those participating.
- Missing participants hurts those who do not participate.
- Incorrect participants (wrong level or expertise) or only slightly better than not participating at all.

- The researcher did not conclude what career level, experience, years of service, or training should participate. The interviewees overwhelmingly answered this question with responses indicating it was person-dependent.

Research Question 2 Findings

Research question two focused on the potential of harm coming from participation. Research question two was: What is the consequence of participating in a tabletop exercise? Does this cause additional risk? The saturation consensus was that although participation improved responsiveness and security, smaller partners may face a disproportionate increase in risk. However, several cases discussed highlighted participation gaps that led to significant security breaches. Participation can increase risk.

Research Question 3 Findings

Research question three asked whether the agenda, goals, and objectives impact the outcome of the tabletop exercise's effectiveness. The resounding response was that all were factors. The more extensive answer here, seen in the observations of the actual tabletop and caught in the interview, was the interrelationship between Research Question 1 and Research Question 3. The sponsoring agency may not care to ensure the correct partners participate. The data was relatively straightforward, and the sponsoring agency is ethically agnostic. They are just as likely to sponsor an event that leaves more problems behind but answers their research question than altruistically trying to improve security.

Unexpected findings

The most significant finding was that the sponsoring agency may be driving issues related to participants and the security of participating. The researcher believed there was a loose connection between agency priorities and other issues. The researcher was surprised that the

issues were as closely related as the research shows. The synergy behind the sponsoring agency causing additional harm to achieve their agenda will likely need further research. If the agency is only interested in its force projection needs for recovery or stabilization, it may not care that there are potentially unintended impacts. These can include publishing data highlighting how more minor businesses play an interconnected role in national security. These smaller stakeholders may only receive negative consequences, even though they walk away feeling better or more protected. The truth is that they may have only highlighted themselves as a target. A small business that one day was hidden and anonymous may be the target of organized crime or state actors just because they participated. The after-action reports or improvements may not help improve security for everyone equally. Additionally, organizational non-compliance emerged as a topic from three interviewees. Understanding that there was a need to implement controls and being unable to do so timely significantly impacted security operations.

Discussion

The research, data, and themes aligned with the empirical and theoretical literature reviewed in Chapter Two. The academic expansion to a new security model is even further confirmed when analyzing issues resolved and analyzed with tabletop exercises.

Current Theoretical Model of the Weakest Link

If the weakest link model described the entire process honestly, identifying the weakest link and improving security would solve the problem, even if momentarily (ASIS, 2010). The Solar Winds attack demonstrates that cybersecurity flaws exist in all security postures. The current security model also does not reflect the positionally dependent relationships (Helbing, 2013). The novel application of the Fractured Flaw model provides a better holistic description of the problem and a numerical result between observed behavior and actual response.

Theoretical Expansion

Fracture mechanics is a branch of materials science and engineering that deals with the behavior of materials containing flaws or defects. Fracture mechanics study how cracks or defects propagate in materials under various conditions. While fracture mechanics is not typically associated with cybersecurity or information security, some conceptual parallels and potential applications more accurately describe the hazards and risks associated with cybersecurity than the weakest link theories. An essential factor to consider is that nearly every company worldwide uses similar or identical software to stop security issues. The software represents a material flaw across every section and subsection before applying the first tension to the material.

In cybersecurity, the analogy between material flaws and vulnerabilities in software or systems. Vulnerabilities are flaws in the design or implementation of software or hardware. Just as fracture mechanics studies how cracks propagate and cause material failures, tabletop exercises study how attackers can exploit vulnerabilities to breach systems or cause failures. The security flaws may often be minor and expand to larger systems (Khan & Abbasi, 2000; Reniers, 2009). Applying fracture mechanics principles to vulnerability assessments causes the analysis of weaknesses in software, networks, and systems; just as fracture mechanics evaluates a crack's critical size and growth, vulnerability assessments aim to determine the criticality and potential impact of a security vulnerability.

Like fracture mechanics inform material safety and maintenance decisions, cybersecurity risk assessments help organizations make informed decisions about mitigating security risks. Organizations can prioritize their security efforts by assessing the likelihood of vulnerability exploitation and the potential impact, similar to prioritizing maintenance based on crack size and

location (Rich 1977). In cybersecurity, patch management is akin to repairing cracks or flaws in a material (Kuna 2013). Regularly applying security patches and updates helps mitigate known vulnerabilities (Vishwanath 2020). Decisions about when and how to apply patches are influenced by factors such as the severity of the vulnerability (analogous to crack size) and the potential impact on operations (Zok 2017).

Engineers and scientists design materials with flaw tolerance or resistance to crack propagation; security professionals can integrate the same concepts into software and system design from the outset. This concept is often called "security by design" or "secure by design." The goal is to minimize the presence of vulnerabilities or flaws in the initial design and architecture (Kuna 2013). Systems and networks can employ intrusion detection and prevention mechanisms to identify and halt potential attacks, akin to identifying and mitigating crack growth in materials (Rich 1977). These mechanisms aim to detect and stop threats early to prevent them from causing significant damage.

Security professionals do not apply fracture mechanics principles in cybersecurity; the underlying concepts of identifying, analyzing, and mitigating flaws or vulnerabilities share similarities. Adopting a better model of risk and threats will allow cybersecurity professionals to prevent more attacks. By using risk assessment, proactive security measures, and effective patch management, organizations can improve their overall cybersecurity posture and reduce the risk of security breaches. Moving past the physical and metaphorical comparisons, the actual value in the comparison is considering the mathematical model of the risk. In the weakest link theory, the risk to the isolated weakest link and its strength. The fractured flaw mechanism of failure considers distributed failures across a material. The same flaw can exist across a computer network or a series of companies. These more closely represent the actual risk. The risk is

distributed and not in a single chain link. The fractured flaw risk for a failure is multiplicative, and the risk calculation is more representative. The distributed dependence extends past the weakest link. The interviews and data analysis showed that many of the issues exploited existed in multiple places, and inclusion or exclusion in prevention activities led to failure or survival.

Implications

There are numerous implications for this research. Using the fracture flaw model will improve overall security for all involved. Using tabletop exercises with historical legacy baggage must be modified to be effective. Security professionals must address organizational non-compliance to cause any improvements from tabletop exercises. The sponsoring agency's responsibility not to harm has to be one of the first considerations. Secondly, identifying the appropriate participants is essential, especially if the goal is not to harm.

Theoretical Implications

Fractured Flaw

Two interviewees added that distributed dependence on each other caused a need for a zero-trust approach or paradigm shift in security. Future security will require a different model that accounts for a connected world that is more complicated than a single connection. The world must recognize that the risks are multiplicative and not isolated.

Pre-supposed Emergency Response

A core fundamental issue was identified by reflecting on the commentary and the data gathered from the analysis of tabletop exercises. The exercises represent the only way stakeholders interplay and work through scenarios to stop cybersecurity issues. The effectiveness of the approach has yielded tremendous results and remains effective. However, one of the most significant drawbacks to the approach is the baggage the approach brings. Most emergency

responders and security professionals arrive at tabletop exercises with a long personal backstory of participation covering their entire careers. Surviving the event, proposing reasonable responses, and taking away lessons learned are great. The tabletop exercise itself provides value in improving cybersecurity. However, the baggage and perceptions from other exercises cloud the actual need. The presupposed response to an emergency deserves cybersecurity as a whole. The larger community coming together for an emergency may not be what is needed and highlights the bigger problem. Cybersecurity events are occurring at an even faster pace than ever anticipated. Only figuring out how the community responds together in an emergency is missing the more significant point. The lack of a community way of strategically growing defense mechanisms wholistically is a challenge that is only beginning to be understood.

Empirical Implications

Organizational Non-Compliance with Security Requirements

Executive Orders, updated laws, and departmental orders now require the inclusion of the insider threat. The insider threat refers to the risk posed to an organization's security, data, systems, or operations by individuals who have authorized access to the organization's resources but use that access maliciously, negligently, or inadvertently. These individuals are typically current or former employees, contractors, or business partners with insider knowledge of the organization's processes and systems (Nam 2019). The insider can break down into Malicious, Negligent, or Compromised Insider. Although a requirement, security, and vulnerability assessors are not incorporating them into any safety basis.

The current published orders require the protection of Operational Technology. Operational Technology (OT) refers to the hardware and software systems used in industrial and manufacturing environments to monitor, control, and manage physical processes and devices.

OT is distinct from Information Technology (IT), which focuses on data processing, networking, and information management within the corporate or business domain. The data shows multiple examples of these issues.

Interviewee one established that his most significant concern was organizational non-compliance. Regardless of how significant improvements were identified or risks- the likelihood of no action may represent an even more substantial risk. The researcher reviewed government requirements for recent changes as a follow-up during the tabletop exercises. Widespread organizational non-compliance is a significant concern. The research highlighted the prevalence of organizational non-compliance. An organizational excuse given for non-compliance is the lack of adoption into the design basis threat or costs. The design basis threat is the threat that a facility must reasonably survive. For most of the government, this design basis threat is a product of the DOD and IC elements and is updated regularly. The researcher conducted a follow-up interview for more information about DBT. The response was that "the DBT stands for Dollar Basis Threat."

Practical Implications

The sponsoring agencies need a cause-no-harm intent and a selfless approach to tabletop exercises. Participation of nearly all parties is voluntary, and the volunteers bear the costs. The larger sponsoring agencies benefit disproportionately from the benefit of smaller players. They need help and support but do little to help the overall security. Researching this topic has led to the conclusion that much of security continues to rely on obscurity rather than active practice. Improving security and protection of vulnerabilities after a tabletop exercise has to be a priority. Risk should not increase after participating.

Another significant finding from the research is that the nature of the tabletop exercise disrupts the intended goals. Cybersecurity and security efforts, in general, are an ongoing effort. The tabletop exercise, by design, is a brief temporal activity. The event carries baggage related to emergency response. These factors may inherently provide a disservice to the intent of the exercise. Although the tabletop exercise represents the implemented method for distributed cyber-security protection efforts, a better approach may be more effective. Future studies should consider using public and private fusion centers explicitly designed for cybersecurity. A challenge to this approach will be the expectation of full-time participants and the increased cost related to security.

The most straightforward recommendation is to include a scenario pre-brief for participants. Based on the longitudinal study with interviewee one, the overall experience improved with a detailed brief before the event. Performing a pre-brief was shown to add value in an Emergency Operations Center setting during a tabletop exercise. Gaining practical value from this input depends on implementing any changes from the tabletop exercise. The opportunity exists to insert this modification into NIMS training (DHS 2008).

Delimitations and Limitations

Delimitations include limiting interviewees to those outside the Department of Defense and Intelligence Communities. Their responses and training are different but represent a much smaller portion of the overall budget and economy. Unlike traditional warfare, they cannot protect the remainder of the population.

Recommendations for Future Research

Future research should consider a controlled series of tabletop exercises that address more variables. Additionally, future researchers will benefit from the information captured in the

original data collection. The historical legacy of tabletop exercises may not be ideal for this application without additional changes.

Other potential gaps that future researchers must investigate include the lack of real-world stress. Tabletop exercises are conducted in a controlled environment, which means they may not fully replicate the stress and chaos of a real crisis. In some cases, tabletop exercise planners design the scenario with the expectation of a successful outcome. The positive outcome by design can lead to unrealistic expectations and an underestimation of the challenges that may arise in an actual incident. Tabletop exercises may focus on a specific scenario while neglecting other essential elements. Ignoring critical factors can create gaps in understanding how different parts of the organization interact during a crisis. In the case of cybersecurity tabletop exercises, the participants must consider all of the technical aspects of systems and network vulnerabilities. Incomplete testing can lead to a false sense of security regarding an organization's cyber resilience. Another area worthy of research is estimating the public's reaction or over-reaction.

Adjacent gaps identified during the interviews was the lack of cross-planning between physical security exercises and cyber security. In real-world events, cyber warfare begins before physical actions. Cybersecurity is a critical component of overall security, including physical security exercises. There are no boundaries between physical and digital security. Two interviewees stated that cybersecurity was excluded from force-on-force exercises. The implications of this oversight have an undetermined effect on overall security.

Summary

This study aimed to evaluate the impact and use of tabletop exercises in preparation for cybersecurity defense in systemized attacks. Research question one was: What is the impact of having the wrong or missing participants in a tabletop exercise? The resounding response was

that not having the correct participants led to multiple issues. The current approach of all participants benefit from participation is incorrect. Having the wrong or missing participants can sabotage the entire training event. Having an absent organization or participant causes complications in response and leads to unrealistic responses.

Research question two was: What is the consequence of participating in a tabletop exercise? Does this cause additional risk? The consensus was that although participation improved responsiveness and security, smaller partners may face a disproportionate increase in risk. Participants risk having their role and significance publicized through the careless publication of tabletop results. The intended goal and purpose of the tabletop events is to improve security. The publication of the interlinked network, highlighting interconnectivity, provides vital information to would-be attackers. The Department of Homeland Security and the Federal Bureau of Investigation have discussed making critical infrastructure information classified. Neither agency has made an official announcement or push for classification, as a large quantity of public information is available.

Research question three asked whether the agenda, goals, and objectives impact the outcome of the tabletop exercise's effectiveness. The resounding response was yes. The link between the negative issues related to the organizational agenda was unexpected. As seen in some of the pre-interview data, there was a slim likelihood that the agency agenda would impact the outcome. Surprisingly, the amount of negative impacts due to the sponsoring agencies' agendas was surprising. The takeaway from this research question is that a seemingly innocent agenda can negatively impact participants. The overall agenda needs to consider a do-no-harm approach to studies. There is overlap with research question two in that failing to protect participants can cause serious harm.

An unexpected finding was the prevalence of corporate non-compliance. Despite having numerous laws, codes, orders, standards, funding, and expectations, many agencies and companies are knowingly non-compliant. The researcher investigated this phenomenon and discovered widespread evidence. The research identified multiple examples and parties that were not compliant but had made an organizational-level decision not to embrace a requirement or standard.

Theoretically, expanding from the weakest link model to the fractured flaw model will significantly improve how risk and survivability affect security arenas. The underlying theory and concepts from the fractured flaw outlay a better mathematical and theoretical approach to evaluating security risks. A weakest link model only addresses which one fails first and does not address the inherent compositions of the systems. A material model such as the fractured flaw addresses security issues, the corresponding material failures, as well as the interconnectivity of the system. The shared resources, such as technology, software, defense technology, and even tabletop exercises, cause every connected chain to have the same weaknesses. The fracture flaw provides a more effective contextualized theory explaining common weaknesses and describing how a security flaw can spread from one area to the next.

REFERENCES

Agboola, F., McCarthy, T., & Biddinger, P. D. (2013). Impact of emergency preparedness exercise on performance. *Journal of Public Health Management and Practice*, 19, S77-S83. https://10.1097/PHH.0b013e31828ecd84

Agner, J. (2021). Tabletop Exercises. *In a guide to healthcare facility dress rehearsal simulation planning: simplifying the complex.* Emerald Publishing Limited.

Aleem, A., Wakefield, A., & Button, M. (2013). Addressing the weakest link: Implementing converged security. *Security Journal*, *26*(3), 236-248. https://doi.org/10.1057/sj.2013.14

Alevizos, L., Ta, V. T., & Hashem Eiza, M. (2022). Augmenting zero trust architecture to endpoints using blockchain: A state-of-the-art review. *Security and Privacy*, *5*(1), e191. https://doi.org/10.1002/spy2.191

Allen, T. R., Crawford, T., Montz, B., Whitehead, J., Lovelace, S., Hanks, A. D., Christensen, A. R., & Kearney, G. D. (2019). Linking water infrastructure, public health, and sea-level rise: Integrated Assessment of flood resilience in coastal cities. *Public Works Management & Policy*, *24*(1), 110–139. https://doi.org/10.1177/1087724X1879838

Angafor, G. N., Yevseyeva, I., & He, Y. (2020, November). Bridging the cyber security skills gap: using tabletop exercises to solve the CSSG crisis. In *Joint International Conference on Serious Games* (pp. 117-131). Springer, Cham. https://doi.org/10.1007/978-3-030-61814-8_10

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/pdf/10.1002/spy2.126

Araz, O. M., & Jehn, M. (2013). Improving public health emergency preparedness through

enhanced decision-making environments: A simulation and survey-based evaluation. *Technological Forecasting and Social Change, 80*(9), 1775-1781. https://doi.org/10.1016/j.techfore.2012.09.018

Arce, I. (2003). The weakest link revisited [information security]. *IEEE Security & Privacy*, *1*(2), 72-76. https://doi.org/10.1002/spy2.126

ASIS International. (2010) Enterprise Security Risk Management: How great risks lead to great deeds: A benchmarking survey and white paper. Alexandria, VA: ASIS International, http://www.asisonline.org/education/docs/CSORT_ESRM_whitepaper_2010-04.pdf.

Batdorf, S. B., & Heinisch Jr, H. L. (1978). Weakest link theory reformulated for arbitrary fracture criterion. *Journal of the American Ceramic Society*, *61*(7-8), 355-358. https://doi.org/10.1111/j.1151-2916.1978.tb09327.x

Bennett, B. T. (2018). *Understanding, assessing, and responding to terrorism: Protecting critical infrastructure and personnel* (2nd ed.). Wiley.

Berghel, H. (2007). Better-than-nothing security practices. *Communications of the ACM*, *50*(8), 15-18. https://doi.org/10.1145/1278201.1278222

Beyer, R., & Sayles, E. (2015). *The Ghost Army of World War II: How One Top-Secret Unit Deceived the Enemy with Inflatable Tanks, Sound Effects, and Other Audacious Fakery*. Chronicle Books.

Blair, J. R., Hall, A. O., & Sobiesk, E. (2019). Educating future multidisciplinary cybersecurity teams. *Computer*, *52*(3), 58-66. https://digitalcommons.usmalibrary.org/usma_research_papers/221/

Boardman, J., & Sauser, B. (2006). System of Systems-the meaning of. In 2006

IEEE/*SMC International Conference on System of Systems Engineering* (pp. 6-pp). IEEE. https:// doi.10.1109/SYSOSE.2006.1652284.

Brajdić, I., Kovačević, I., & Groš, S. (2021). Review of national and international cybersecurity exercises conducted in 2019. *ICCWS 2021 16th International Conference on Cyber Warfare and Security* (p. 28). Academic Conferences Limited. https://doi.10.34190/IWS.21.034

Brunner, J., & Lewis, D. (2006). Tabletop exercises can train all the staff for safety. *The Education Digest, 72*(4), 46-49. https://eric.ed.gov/?id=EJ769399

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS* quarterly, 523-548.

Busby, J. W., Baker, K., Bazilian, M. D., Gilbert, A. Q., Grubert, E., Rai, V., ... & Webber, M. E. (2021). *Cascading risks: Understanding the 2021 winter blackout in Texas.* Energy Research & Social Science, 77, 102106. https://doi.org/10.1016/j.erss.2021.102106

Cantelmi, R., Di Gravio, G., & Patriarca, R. (2021). Reviewing qualitative research approaches in the context of critical infrastructure resilience. *Environment Systems and Decisions*, 136. https://doi.org/10.1007/s10669-020-09795-8

Chandra, A., Williams, M. V., Lopez, C., Tang, J., Eisenman, D., & Magana, A. (2015). Developing a tabletop exercise to test community resilience: Lessons from the Los Angeles County Community Disaster Resilience Project. *Disaster Medicine and Public Health Preparedness, 9*(5), 484-488. http://dx.doi.org/10.1017/dmp.2015.99

CISA (2020). *National Infrastructure Protection Plan*. Accessed at: https://www.cisa.gov/national-infrastructure-protection-plan.

Connelly, L. M. (2016). Trustworthiness in qualitative research. *MedSurg Nursing*, *25*(6), 435. https://link.gale.com/apps/doc/A476729520/AONE?u=googlescholar&sid=bookmark-AONE&xid=d5cf03d0

Davies, F., Veloutsou, C., & Costa, A. (2006). Investigating the influence of a joint sponsorship of rival teams on supporter attitudes and brand preferences. *Journal of Marketing communications, 12*(1), 31-48. https://doi.org/10.1080/13527260500264574

Dawson, M., Bacius, R., Gouveia, L. B., & Vassilakos, A. (2021). Understanding the challenge of cybersecurity in critical infrastructure sectors. *Land Forces Academy Review*, *26*(1), 69-75. https://sciendo.com/downloadpdf/journals/raft/26/1/article-p69.xml

Davis, R., & Pease, K. (2000). Crime, technology, and the future. *Security Journal*, *13*(2), 59-64. https://repository.lboro.ac.uk/articles/journal_contribution/Crime_technology_and_the_future/9580442

Dausey, D.J., Buehler, J.W. & Lurie, N. Designing and conducting tabletop exercises to assess public health preparedness for artificial and naturally occurring biological threats. *BMC Public Health,* **7,** 92 (2007). https://doi.org/10.1186/1471-2458-7-92

Department of Homeland Security (2008). *National Incident Management System Report.* https://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf

Dorn, T. M. (2020). *Phenomenological Study Examining the Vulnerability of U.S. Nuclear Power Plants to Attack by Unmanned Aerial Systems* (Order No. 28154029). https://www.proquest.com/openview/081ddae7bac7627d699be3d8d335f1d4/1?pq-origsite=gscholar&cbl=18750&diss=y

Easton, K. L., McComish, J. F., & Greenberg, R. (2000). Avoiding common pitfalls in

qualitative data collection and transcription. *Qualitative health research, 10(5), 703-707. https://doi.org/10.1177/104973200129118651*

Erickson, Andrew (2019). *3 SCADA traffic control and automation strategies*. Retrieved 18 January 2020. https://www.dpstele.com/insights/2019/07/18/3-scada-traffic-control-automation-strategies/

Executive Order (2013). Executive Order -- Improving critical infrastructure cybersecurity, Feb 12, 2013. https://www.dhs.gov/publication/executive-orders-13636-and-13691-privacy-and-civil-liberties-assessment-reports

Federal Emergency Management Agency (N.D.). Emergency management institute. Unit 11: Course training. [http://www.training.fema.gov/EMIWEB/downloads/is139Unit11.doc].

Fontes, R. L., Korn, E., Fletcher, D., Hillman, J., Mitchell, E., & Whitham, S. (2020). Jack Voltaic®. *The Cyber Defense Review*, *5*(3), 45-56. https://cyberdefensereview.army.mil/Portals/6/Documents/2020_fall_cdr/2020_fall_cdr_full.pdf

Fox, D. B., McCollum, C. D., Arnoth, E. I., & Mak, D. J. (2018). *Cyber wargaming: Framework for enhancing cyber wargaming with realistic business context*. Mitre Corp, Mclean, VA. https://apps.dtic.mil/sti/pdfs/AD1108071.pdf

Freeman, S. G., St Michel, C., Smith, R., & Assante, M. (2016). Consequence-driven cyber-informed engineering (CCE) (No. INL/EXT-16-39212). Idaho National Lab. (INL), Idaho Falls, ID (United States). https://doi.10.2172/1341416

Frey, S., Rashid, A., Anthonysamy, P., Pinto-Albuquerque, M., & Naqvi, S. A. (2017). The good, the bad and the ugly: A study of security decisions in a cyber-physical systems game. *IEEE Transactions on Software Engineering*, *45*(5), 521-536. https://research-information.bris.ac.uk/en/publications/the-good-the-bad-and-the-ugly-a-study-of-

security-decisions-in-a--2

Glesne, C. (2014). Becoming qualitative researchers: An introduction (5th ed.). Pearson.

Gupta, S., Schreiber, M., McGuire, T., & Newton, C. (2021). Addressing pediatric mental health during COVID-19 and other disasters: a national tabletop exercise. *Disaster Medicine and Public Health Preparedness*, 1-13. https://pubmed.ncbi.nlm.nih.gov/33867004/

Hatzivasilis, G., Soultatos, O., Ioannidis, S., Verikoukis, C., Demetriou, G., & Tsatsoulis, C. (2019, May). Review of security and privacy for the Internet of Medical Things (IoMT). In 2019 *15th international conference on distributed computing in sensor systems* (DCOSS) (pp. 457-464). IEEE. https://ieeexplore.ieee.org/abstract/document/8804790

Hirshleifer, J. (1983). From weakest-link to best-shot: The voluntary provision of public goods. *Public Choice*, *41*(3), 371-386. https://doi.org/10.1007/BF00141070

Holloway, L. G. (2007). Emergency preparedness: Tabletop exercise improves readiness. *Professional Safety*, *52*(8), 48. https://www.proquest.com/openview/85b7264a708d0cd46edd2bad8c1c4f31/1?pq-origsite=gscholar&cbl=47267

Irwin, Luke (2019). How long does it take to detect a cyber attack? IT Governance, March 14, 2019. Retrieved February 10, 2020. https://www.itgovernanceusa.com/blog/how-long-does-it-take-to-detect-a-cyber-attack

Johnson, Leighton (2019). Security Controls Evaluation, Testing, and Assessment Handbook (Second Edition), *Academic Press,* 2020. doi.org/10.1016/B978-0-12-818427-1.02001-2.

Jorgenson, D. W., & Stiroh, K. J. (1999). Information technology and growth. *American Economic Review*, *89*(2), 109-115. https://doi.org/10.1257/aer.89.2.109

Kim, S., Ramkumar, M. & Subramanian, N. (2019). Logistics service provider selection for disaster preparation: A socio-technical systems perspective. *Ann Oper Res* 283, 1259–1282. https://doi.org/10.1007/s10479-018-03129-3

Korn, E. B., Fletcher, D. M., Mitchell, E. M., Pyke, A. A., & Whitham, S. M. (2021). Jack Pandemus–Cyber incident and emergency response during a pandemic. *Information Security Journal: A Global Perspective*, *30*(5), 294-307. https://doi.org/10.1080/19393555.2021.1980159

Kuna, M. (2013). Finite elements in fracture mechanics. *Solid mechanics and its applications*, 201, 153-192, ASM International, Materials Park, Ohio.

Lawn, B. (1993). *Fracture of Brittle Solids* (2nd ed., Cambridge Solid State Science Series). Cambridge: Cambridge University Press. doi:10.1017/CBO9780511623127

Lasky, Mary. (2010). "The value of tabletop exercises and one-page planning documents." *Journal of Business Continuity & Emergency Planning 4* (2), 132-141. https://hstalks.com/article/4078/the-value-of-tabletop-exercises-and-one-page-plann/

Lee, L. (2019). Cybercrime has evolved: It's time cyber security did too. *Computer Fraud & Security*, *2019*(6), 8-11. https://doi.org/10.1016/S1361-3723(19)30063-6

Loeb, Larry (2016). Researchers find VoIP phones vulnerable to simple cyber-attacks, security Intelligence, February 22, 2016. https://securityintelligence.com/news/researchers-find-voip-phones-vulnerable-to-simple-cyberattacks/

McGee, S., Frittman, J., Ahn, S. J., & Murray, S. (2016). Implications of cascading effects for the Hyogo Framework. *International Journal of Disaster Resilience in the Built Environment, 7*(2), 144-157. https://doi-org.ezproxy.liberty.edu/10.1108/IJDRBE-03-2015-0012

Minei, E., & Matusitz, J. (2011). Cyberterrorist messages and their effects on targets: A qualitative analysis. *Journal of Human Behavior in the Social Environment, 21*(8), 995-1019. doi:10.1080/10911359.2011.588569

Mirea, M., Wang, V., & Jung, J. (2019). The not-so-dark side of the darknet: a qualitative study. *Security Journal, 32*(2), 102-118. https://www.researchgate.net/publication/326489545_The_not_so_Dark_Side_of_the_Darknet_-_A_Qualitative_Study

Mishra, S., Sankar Mahapatra, S. and Datta, S. (2014), "Agility evaluation in fuzzy context: Influence of decision-makers' risk bearing attitude", *Benchmarking: An International Journal*, *21*(6), 1084-1119. https://doi.org/10.1108/BIJ-04-2012-0026

Mitchell, E. M. (2020). *Cyber Security @ home: The effect of home user perceptions of personal security performance on household IoT security intentions* (Order No. 27959802). https://www.proquest.com/dissertations-theses/cyber-security-home-effect-user-perceptions/docview/2429880370/se-2?accountid=10478

Mitchell, E., Fletcher, D., Korn, E., Whitham, S., Hillman, J., Yearwood, R., ... & Hruska, R. (2021). Jack Voltaic 3.0 cyber research report. https://digitalcommons.usmalibrary.org/cgi/viewcontent.cgi?article=1048&context=aci_rp

Monika et al. (2016). "Experimental analysis of ransomware on Windows and Android platforms: evolution and characterization. The 2nd international workshop on future information security." Privacy & Forensics for Complex Systems. *Procedia Computer Science, 94,* 465–472. doi.org/10.1016/j.procs.2016.08.072

Moore, E., Fulton, S., & Likarish, D. (2017, May). Evaluating a multi-agency cyber security training program using pre-post event assessment and longitudinal analysis. In *IFIP World Conference on Information Security Education,* 147-156. doi:10.1007/978-3-319-

58553-6_13

Mueller III, R. S. (2005). Working with our neighbors all over the world. *Vital Speeches of the Day*, *71*(21), 645. https://archives.fbi.gov/archives/news/speeches/collections/2013-speeches

Murphy, P. J., & Borghard, E. (2020). To defend forward, U.S. cyber strategy demands a cohesive vision. *The Cyber Defense Review*, *5*(3), 15-30. https://cyberdefense review.army.mil/Portals/6/Documents/2020_fall_cdr/CDR%20V5N3%2002_Murphy_Borghard.pdf?ver=SGIrAHDc1d3ZOrQihG_XFg%3D%3D

Nam, T. (2019). Understanding the gap between perceived threats to and preparedness for cybersecurity. *Technology in society*, *58*, 101122. doi.org/10.1016/ j.techsoc.2019.03.005

National Research Council. (2005). *Improving evaluation of anticrime programs*. Washington, DC: The National Academies Press. http://www.nap.edu/catalog.11337.html

Nazir, H. (2021). Lessons Learned from the February 2021 Texas Power Outage. *CERI Electricity Report*. https://ceri.ca/assets/files/Electricity%20Commodity%20 Update_April%202021.pdf

Oo, M. K., Siswoyo, B. E., Thit, W. M., & Thajeen, J. (2021). *A guideline for innovative tabletop & simulation exercise.* https://mbdsnet.org/wp-content/uploads/2021/04/Guideline-for-Innovative-Tabletop-Simulation.pdf

Ota, Y., Mizuno, E., Watari, T. (2022). Development of a hybrid exercise for organizational cyber resilience. *Safety and Security Engineering IX*, 206, 55. https://www.witpress.com/elibrary/wit-transactions-on-the-built-environment/206/38201

Paul, Deanna (2019). "*Charter flight from Guantanamo Bay skids off runway and winds up in a Florida river*" The Washington Post. May 4, 2019.

Paris, Costas (2019). "Coast Guard finds four trapped crew members in capsized cargo ship." The Wall Street Journal. September 9, 2019. https://www.wsj.com/articles/coast-guard-searches-for-four-after-cargo-ship-capsizes-near-georgia-port-11567982240

Petit, F. D. P., Bassett, G. W., Black, R., Buehring, W. A., Collins, M. J., Dickinson, D. C., ... & Peerenboom, J. P. (2013). *Resilience measurement index: An indicator of critical infrastructure resilience* (No. ANL/DIS-13-01). Argonne National Lab.(ANL), Argonne, IL https://publications.anl.gov/anlpubs/2013/07/76797.pdf

Pfeifer, J. W. (2018). Preparing for cyber incidents with physical effects. *The Cyber Defense Review, 3*(1), 27–34. http://www.jstor.org/stable/26427372

Russell, S. (2020). Trusted CI Webinar: Cybersecurity Maturity Model Certification (CMMC). https://www.ideals.illinois.edu/items/116030

SCCIC, South Carolina Critical Infrastructure and Intelligence Center. (2021). Ransomware and Social Engineering Enduring Threats to South Carolina State, Local, and Critical Infrastructure Networks. *Field Analysis Report,* DHS-IA-FAR-2021-16214, October 29, 2021.

Savoia, E., Biddinger, P. D., Fox, P., Levin, D. E., Stone, L., & Stoto, M. A. (2009). Impact of tabletop exercises on participants' knowledge of and confidence in legal authorities for infectious disease emergencies. *Disaster medicine and public health preparedness*, *3*(2), 104-110. https://www.cambridge.org/core/journals/disaster-medicine-and-public-health-preparedness/article/abs/impact-of-tabletop-exercises-on-participants-knowledge-of-and-confidence-in-legal-authorities-for-infectious-disease-emergencies/04C7BCE3F14541A892323B0EBD3939E3

Shore, M., Zeadally, S., & Keshariya, A. (2021). Zero trust: The what, how, why, and when.

Computer, 54(11), 26-35. doi.org/10.1109/MC.2021.3090018.

Shreeve, B., Hallett, J., Edwards, M., Anthonysamy, P., Frey, S., & Rashid, A. (2020). "So if Mr. Blue Head here clicks the link..." Risk thinking in cyber security decision making. *ACM Transactions on Privacy and Security (TOPS)*, *24*(1), 1-29. https://dl.acm.org/doi/abs/10.1145/3419101

Stone, Mark (2023). How Much is the U.S. Investing in Cyber (And is it Enough)? *Security Intelligence*, January 20, 2023. https://securityintelligence.com/articles/how-much-is-us-investing-in-cyber/

Tsuchiya, A., Ota, Y., Takayama, Y., Aoyama, T., Hamaguchi, T., Hashimoto, Y., & Koshijima, I. (2018). Cyber incident exercise admitting inter-organization for critical infrastructure companies. *In Computer Aided Chemical Engineering,* 44, 1645-1650. https://nrid.nii.ac.jp/en/nrid/1000080314079/

Verner, D., Petit, F., & Kim, K. (2017). Incorporating prioritization in critical infrastructure security and resilience programs. *Homeland Security Affairs, Xiii.* https:// www.proquest.com%2Fscholarly-journals%2Fincorporating-prioritization-critical%2Fdocview%2F2203199980%2Fse-2%3Faccountid%3D12085

Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*, 128, 113160. https://doi.org/10.1016/j.dss.2019.113160

Vito, G. F., & Higgins, G. E. (2015). *Practical program evaluations for criminal justice.* New York, New York, United States of America: Routledge, Taylor, and Francis Group.

Weber, R. (2018). DOD's deputy CIO highlights initial steps in addressing emerging cyber risks. *Inside the Army*, *30*(45), 9-10. https://cyberdefensereview.army.mil/Portals

/6/CDR_V3N2_SUMMER-2018_Complete.pdf?ver=2018-09-06-092054-633

Wells, W. (2007). Type of contact and evaluations of police officers: The effects of procedural justice across three types of police-citizen contacts, *Journal of Criminal Justice, 35*(6), 2007, 612-621. https://doi.org/10.1016/j.jcrimjus.2007.09.006.

Wendelboe, A. M., Amanda Miller, J. D., Drevets, D., Salinas, L., Miller, E. J., Jackson, D., ... & Public Health Working Group. (2020). Tabletop exercise to prepare institutions of higher education for an outbreak of COVID-19. *Journal of Emergency Management, 18*(2), 1-20. https://doi.org/10.5055/jem.2020.0463.

Whelan, C. (2021). Texas Death Toll In February's Winter Storm Nearly Doubles To 111. https://www.npr.org/2021/03/26/981594093/texas-death-toll-infebruarys-winter-storm-nearly-doubles-to-111

Fennelly, L. J., & Perry, M. A. (2020). Building a sustainable culture of security. *In The Professional Protection Officer*, 397-401. Butterworth-Heinemann. https://www.sciencedirect.com/science/article/pii/B9780128177488000353

Fisher, R. E., Bassett, G. W., Buehring, W. A., Collins, M. J., Dickinson, D. C., Eaton, L. K., ... & Peerenboom, J. P. (2010). Constructing a resilience index for the enhanced critical infrastructure protection program (No. ANL/DIS-10-9). Argonne National Lab. (ANL), Argonne, IL (United States). Decision and Information Sciences. https://doi.org/10.2172/991101

Moteff, J., & Parfomak, P. (2004, October). Critical infrastructure and key assets: Definition and identification. Library of Congress Washington DC Congressional Research Service.

Kitchin, R., & Dodge, M. (2020). The (in) Security of smart cities: Vulnerabilities, risks,

mitigation, and prevention. In *Smart Cities and Innovative Urban Technologies* (pp. 47-65). Routledge.

Rich, Thomas P., Peter G. Tracy, and David J. Cartwright. "A survey of fracture mechanics applications in the United States." *Engineering Fracture Mechanics* 9, no. 2 (1977): 341-360.

Schlanger, K., Black, J. M., Smith, M., Ridpath, A., Crause, C., Holderman, J. L., ... & Kirkcaldy, R. D. (2021). Enhancing U.S. local, state, and federal preparedness through simulated interactive tabletop exercises of a mock antibiotic-resistant gonorrhea outbreak, 2018–2019. *Sexually Transmitted Diseases*, *48*(12), S174-S179.

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. Future Internet, 13(2), 39. https://doi.org/10.3390/fi13020039

Zok, F. W. (2017). On weakest link theory and Weibull statistics. *Journal of the American Ceramic Society*, *100*(4), 1265-1268. https://doi.org/10.1111/jace.14665

APPENDICES

Appendix A

Relationship Between Research Questions and Interview Questions

Interview Question	Attribute / Background Question	Research Question 1	Research Question 2	Research Question 3
1. Please introduce yourself to me as if we had just met one another.	P			
2. Please walk me through your background in cybersecurity or tabletop exercises.		P	P	
3. Describe your role and background in cybersecurity.	P			
4. How does your division fit into the bigger picture of critical infrastructure?	P			S
5. What are your recent training exercises?	P			S
6. Have you or your division experienced a cyber attack?	P		P	
7. Has any of the support infrastructure up or downstream been affected by cyber incidents?		P	P	S
8. Have you declined a tabletop exercise or another training event? Why?			P	S
9. Have the tabletop exercises you participated in been helpful?			P	S
10. Who was the sponsoring agency, and what do you know about their overall purpose?				P
11. How well were you prepared for your role in the tabletop exercise? Were you able to add value?		P		
12. Was there another participant (or participants) struggling to fulfill their role?		P		
13. What questions or value were you able to add?		P		
14. As a group, where were there questions or sections left out? Did a fill-in play a sector's role during the scenario?		P		
15. Did any groups disagree over a response due to similar scope or roles?		P		
16. Following the tabletop exercise, were any changes made to your organization?			P	S
17. Have you had any cyber incidents since the exercise? Did the exercise help in any way?			P	S
18. This next question is unique in that it will invite you to look ahead. How will your organization participate in the future? Is there another alternative?		S	P	S
19. We've covered a lot of ground in our conversation, and I appreciate your time. One final question: What else would be vital about tabletop exercises?	P	S	S	S
P -Primary Connection				
S -Secondary Connection				

Appendix B

Survey Results and Summary

Survey Questions:

1. Name (if you wish to provide it)?
2. Organization (If you wish to provide it)?
3. Size
    a. Less than 100
    b. 100-500
    c. More than 500
4. Is your agency or company: (pick one)
    a. Private/Commercial
    b. Local/Municipal Government
    c. State Government
    d. Federal Government
5. Have you participated in a tabletop emergency preparedness exercise?
6. Have you participated in a cybersecurity-related tabletop exercise?
7. In general, was the tabletop exercise beneficial to your agency/company?
8. Did you feel the exercise included the right topics to help meet the protection goals?
9. Did your exercise miss participants or were stand-ins used for missing organizations?
10. Do you know of anyone being attacked closely following participation in an exercise?
11. Would you be willing to participate in a follow-up interview? (please provide contact info)