Summer 2019

A cyber focused table top exercise for Iowa State University

Christopher Garrison

My Iowa State University Creative Component: A Cyber focused Table Top exercise for Iowa State University

by

Chris Garrison

A creative component submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

MASTER OF SIENCE

Major: Information Assurance

Program of Study Committee:
Doug Jacobson, Major Professor

Iowa State University

Ames, Iowa

2019

TABLE OF CONTENTS

ACKNOWLEDGMENTS

I would like to thank my major professor Doug Jacobson for his guidance and support throughout the course of this research.

In addition, I would also like to thank my friends, colleagues, the department faculty and staff for making my time at Iowa State University a wonderful experience.

ABSTRACT

Many departmental organizations rely on the digital space more and more. For the purposes of responding to and mitigating a cyber event, these departments need to communicate with one another and bring their full potential to react. One of the commonly used tools is the Table Top Exercise. This type of solution has been successfully used to prevent public health emergencies.

When it comes to cyber events, there is a lack in the cyber component of many Table Top Exercises. Therefore, we designed a cyber focused Table Top Exercise.

CHAPTER 1. CYBER FOCUSED TABLE TOP EXERCISE

Relevant Definitions

- Table Top: A professional exercise where disaster scenarios are simulated and responded to.
- Cyber Event: Any unwanted event that takes place in the cyber space that would require a response.
- Cyber Space: A scope or field involving digital infrastructure.
- VPN (Virtual Private Network): A simulated computer network that can be segregated and restricted from standard networks. Usually these are hosted on one or more servers.
- Splunk SIEM: Security Information and Event Management
- Elk stack: Elasticsearch, Logstash, Kibana

What is a Table Top Exercise?

A Table Top is a disaster scenario walk through that involves the professionals that would be responsible for responding to said disasters. The purpose is to walk through these scenarios and to analyze procedures, responses and communication of the different organizations and departments that are responsible for dealing with these problems. They usually involve professionals from many different areas that must work together to solve problems.

What does a Table Top focus on?

Most Table Tops focus on disasters that create time critical problems to solve. How long until food or gas runs out? When can we deliver help and supplies over a certain distance? How long will it take to get power back on? These questions have answers based on experience and on

the simple fact that we know speed, distance and therefore time. We can measure current supplies. We know how long it will take to deliver supplies. We know how much personnel we have and how much will be needed.

Why would we need to change?

However, as we rely more and more on digital infrastructure, we face new challenges. These challenges are not only different than what has been encountered in the past but also unpredictable. It is difficult to determine how much time it will take to solve problems in the digital space. Also, the nature of these problems can make it difficult to detect when they have started.

How can we address this?

To address the need for a digital space disaster exercise, we need to create a cyber focused Table Top. This new format will not just focus on timely responses and deployment of resources but will focus on measuring communication protocols and examination of standard operating procedures.

Iowa State Cyber focused Table Top.

In the following, we will discuss designing a Table Top exercise designed around Iowa State University. This is intended to be a high-level design that can later be tailored to the specific needs and organization on the university at the time of future implementation.

CHAPTER 2. IOWA STATE CYBER FOCUSED TABLE TOP EXERCISE

Schedule for the Day.

- **Pre-Game Briefing** – Donuts and coffee, what are the expectations, this is not an assessment
- **Game Start** – Get into positions, start the game
- **End Game Debriefing** – Tell all by all teams
- **After Action Report** – Two weeks later, White Team creates a report, no names, summery of context and provide perspective, create insight

It is important to note at the beginning that this is not an assessment. No one person or group will be evaluated. That is not the purpose of a Table Top. The final report will not include names and will be anonymous.

What does this Cyber focused Table Top consist of?

- **Participants** – Professionals that work in the various departments or major organization
- **Resources** – Facilitators, observers and technology
- **Set up** – The organization and placement of resources as to facilitate the normal day to day operations of the participants
- **Expectations** – To simulate normal operations for the participants and for them to be confronted with various Cyber based Incidents
- **Results** – To uncover ambiguities in procedures and to test the communication suit between the participants

Iowa State's main players.

Participants – Blue team

- **Major Organizations** – Colleges, Parks library, Thielen Student Health Center, etc.
- **Iowa State IT Services** – This is the main IT support for Iowa State University and its major organizations

These are the major players. Major organizations can be anyone or any group that plays a major role. Also, they can be any group that plays a large role in interdepartmental communications.

Iowa State's Support Staff.

Resources – Facilitators and Observers

- **White team** – group of observers, one in every room, game master
- **Red team** – will run the scenarios
- **Miscellaneous support staff and assistants (green team)** – will fill in the gaps, example: answer the phone for the police line or act as a 3rd party that is involved in a scenario, there may be a green team coordinator

White team should be present with every group. They should record all perinate data that will allow them to accurately recreate events and the responses to those events.

Red team will run a predetermined, scheduled series of events. This can be attacks to the network or even calling in an event to a specific department. Also, red team has access to the network as needed. This will allow for log entries and other log/event trail generation. Red team

will not deviate from the script, for example: red team will not actively try to break in or alter resources other then what has been indicated in the script.

Who is Running the Show?

- **The Game Master** – Part of the white team, knows everything and will direct and guide as needed, major purpose is to deal with the unexpected; keep up the momentum; and keep the game on track
- **Green Team coordinator** – Helps out the green team by assisting with dialog and improvising what is needed

The Game Master (GM) will be in charge of keeping the game going forward. The GM will try to solve any unforeseen problems that might occur after the game has started. The Green Team coordinator is optional. This position will be needed if a scenario requires a lot of support and a coordinator is required.

Who Knows What?

- **White Team** – Knows everything, has access to all teams
- **Red Team** – Knows what is in the event script
- **Blue Team** – Knows what Red and Green Team lets them know
- **Green Team** – Knows what they are told by facilitators
- **Designers** – Know everything

Iowa State's Physical/Software Infrastructure.

Resources – Technology

- **Equipment and Hardware** – Server, Virtual Machines, Computers, a closed Local Area Network, Local phone system
- **Software and Applications** – ESXi Hypervisor, Splunk SIEM, Email server, Operating systems and application that users normally use for everyday tasks, Elk stack
- **Scenario Specific** – Examples: rouge access point, bitcoin mining traffic generator, shadow IT servers
- **White Team Observation Tools** – Tools that allow White Team to better record data for later review. This can be phone loggers, screen captures, recording devices etc.

Iowa State's Basic Set Up Requirements.

Set up – In general

- **Rooms** – All participants should be separated by rooms. This will facilitate communication via email and the phone system.
- **Computers** – All participants need a computer to access the Table Top network. They will then access their appropriate virtual machines that will act as their work place computers. Also, a VPN that allows them to access information from the web.
- **Phone System** – The phone system will use real world phone numbers on a closed local phone network.

Set up – Some specifics

- **Phones** – Local phone system cut off from the rest of the world, a phone in every room for every team and group, use real world phone numbers that teams can look up in the real world
- **VPN** – Allows access to the same resources as would be in normal operations (such as phone numbers)
- **SIEM** – Duplicate incoming traffic and SIEM events to the local network simulating normal operations

Customizations?

Different configurations will be created as needed. If a scenario needs something different (example: legal) then teams and resources can be adapted. If the scenario requires a real FBI agent, then get one. If the scenario doesn't expect one, then Green team should improvise.

Expectations for Iowa State.

The expectation is that we simulate a standard working day for the participants as closely as possible. We will simulate network traffic and activities. Create access logs that one would expect in normal daily operations. Over all just another day at work.

Then, red team will initiate preplanned events that the participants will need to address. This should show us how the participants currently deal with problems that occur in the digital space.

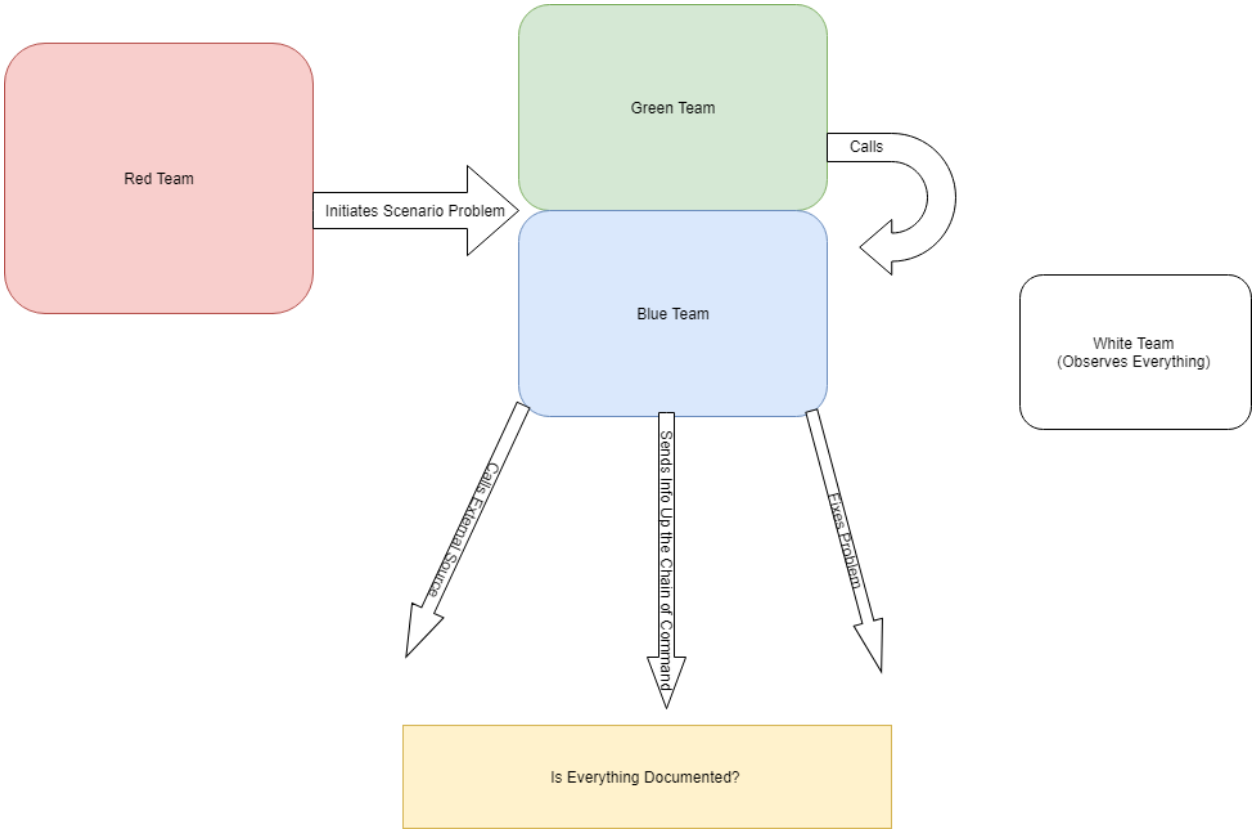

Figure 1 Table Top Abstract

Results for Iowa State.

End game debriefing

- **White team report** – The observers will report what they saw
- **Red team reveals** – The red team will explain their actions
- **Compare notes** – All teams will give their reaction to the exercise
- **Suggestions** – A discussion involving everyone

The results should uncover ambiguities in procedures and create debate about communications between the participants. Red Team and Green Team will reveal their roles and event actions. Then, each major organization will present their experiences and discuss any problems they may have encountered. White Team will review any initial reaction and insights. Finally, White Team will create an inclusive anonymous report along with suggestions and other forms of insight and make it available to all who participated.

CHAPTER 3. Conclusion

In conclusion a Cyber focused Table Top will allow security professionals to be more aware of their response potential. It will create interdepartmental understanding. Also, allow for an over all review of an organizations readiness and reveal areas that might need adjustment. Finally, it will exercise and test communication protocols between all the entities involved.

References

Beese, Zach. Interview. Chris Garrison. March 2019. in person.

Lohrbach, Michael. Interview. Chris Garrison. 14 February 2019. in person.

VMware. *vmware.com*. 2019. April 2019.