Disgruntled Graduate Student

1. Tabletop Exercise Instructions

1.1. Who Needs to Do What in a Tabletop Exercise?

For a Tabletop Exercise there are three potential roles: Participant, Facilitator, and Evaluator. Both the Participant and the Facilitator are mandatory, while the Evaluator can be thought of as an "outside" participant that can be helpful in larger Tabletop Exercises. While the minimum number of people required is 1 (the Participant and Facilitator as the same person), it is more effective to have a separate Facilitator.

Participant's Role

The Participant is the person who will be involved in the Tabletop Exercise. They should be someone who would be involved in an actual event that the Tabletop Exercise is modeling. Therefore, it is best to gather as many people that have a relation to the modeled event as possible to drive the best outcomes.

Facilitator's Role

The Facilitator is the guide for the Tabletop Exercise. Their role is to read through the initial prompt, drive the conversation to productive answers, and add appropriate Injects as required. They may pose questions to the Participants, either from the Tabletop Exercise document, or of their own, as well as ensure the prompt is clear and scope the prompt as needed. It is best to have a Facilitator that who is familiar with the situation and topics. They do not necessarily need to be someone who would be directly involved to free up Participant slots for those closest to the actual event the Tabletop Exercise is modeling.

Evaluator's Role

The Evaluator is responsible for keeping notes on the progress of the Tabletop Exercise. While not necessary, they can play a key role as an "outside observer" to the Tabletop Exercise. They should not prompt Participants or interfere unless they notice a hazard to the current Participants. Any interjections from them must be though the Facilitator, who has the option to bring up their comment. Evaluators can be complete outsiders to the situation or simulated event, both to free up Participants and to provide more objective evaluation of the Tabletop Exercise. Evaluators are expected to summarize their observations at the end of the Tabletop Exercise.

1.2. What is the Purpose of a Tabletop Exercise?

A Tabletop Exercise is a tool to facilitate role play of a scenario, similar to simulating an experiment before conducting it. While the purpose is tailored to each scenario, broadly speaking the goal is to evaluate current plans and procedures, and to determine risks and hazards. By testing out current plans and procedures (or approximations if there are not currently any), the participants are able to determine their current preparedness level. The injects and questions, either generated by the Facilitator or take from the Tabletop Exercise, are targeted at determining worst case scenarios to help achieve best case preparedness levels.

Simply put it is natural, and even encouraged, to fail miserably in the Tabletop Exercise. For the same reason that it is far cheaper to simulate an experiment before conducting it, it is best to find weaknesses in a

Tabletop Exercise and correct them so if the scenario becomes a reality, you are ready.

1.3. Where Does a Tabletop Exercise Take Place?

A Tabletop Exercise should use a plausible scenario for every simulation. The Facilitator may modify minor details in an exercise to better suit a particular situation, but all expectations should be reasonable. For example, if it is not reasonable or practical to have a duplicate lab elsewhere, then it should not be considered a viable option during the Tabletop Exercise.

As for physical location, a Tabletop Exercise can take place anywhere, even virtually. It is best to choose a location that is quiet and without distractions, to allow a focused and non-threatening environment. However, if physical system or location based questions could occur (such as where is this building's tornado shelter), it may be preferable to conduct a Tabletop Exercise on location to generate the most accurate findings.

1.4. When Should Tabletop Exercises Be Conducted?

The initial Tabletop Exercise can be conducted at will, although it is best to do so before the event it describes happens. Once the exercise has been conducted, it should be determined in the Hot Wash when the exercise should be conducted again. Generally it is best to conduct exercises every year or two, or when there is a major change in policy, personnel, or organization structure, to ensure findings from a previous exercise are not out of date.

1.5. Why are Tabletop Exercises Important?

There are multiple reasons to conduct a Tabletop Exercise. First, it is an excellent method to determine and mitigate human issues associated with unplanned events. Brainstorming plans ahead of time allows you to have the best case preparedness level and clarity when reacting to an event.

Second, it ensures that all of the parties involved in the Tabletop Exercise can voice diverse ideas and viewpoints. Frequently the topics covered are situations we have not or do not want to think about, but by completing the exercise we help to ensure the continuity of our research and safety of those involved.

Third and finally, it should be fun and build camaraderie among the participants.

1.6. How to Conduct a Tabletop Exercise?

The Tabletop Exercise is a facilitated exercise. The Facilitator will read each section, starting with the Incident Notification, followed by each Inject, one after another. At each stop in the scenario, the Participants will then review and discuss the Inject as a group. This group discussion should engage **all** members and everyone should have the opportunity to provide constructive feedback to develop solutions to the issues presented.

The following tips should be observed by all Participants:

- Do not attack others! Remember, the goal is to be open-minded. As long as the suggestion is on topic, brainstorming is about building up ideas, not tearing people down. The Facilitator should do their best to make the environment open and constructive.
- Do not rush! The Incident Notification section should take at least 5 minutes, each Inject 15-30 minutes, and the Hot Wash section 20-30 minutes. Plan time accordingly to make sure each topic can be explored properly.
- Do not cheat! It is okay to fail in the Tabletop Exercise, so do not cheat by looking things up or using outside resources. If you have an existing plan to manage this or a similar issue, you may bring

and follow that. If you do not have a plan, make that an action item in your Hot Wash.

- Do not forget solutions! While the problem or issue may be jarring, it is imperative that solutions come out of the Tabletop Exercise. Therefore, focus on solutions and recommendations to achieve best case preparedness.
- Do not fight scenario! While the Facilitator may have made some slight modifications to make the Tabletop Exercise fit your organization, Participants should follow the scenario. It might seem funny or unreasonable, but each of these exercises is based on a real event. Therefore, resist the temptation to change the narrative.

2. Exercise

2.1. Exercise Objectives

This exercise was designed to focus on the following objectives:

- Identify options to assist students who are in a fragile emotional state,
- Identify potential weaknesses in a group's disaster recovery (DR) ability, and
- Develop communication plans and access controls to mitigate rouge actors.

2.2. Incident Notification

Towards the end of a semester you receive news, directly or indirectly, that a current Graduate Student in your lab has received a poor mark on an exam. The student attributes the bad mark to you personally, having been required to work long hours in the lab the week before the exam. This student is a key member of your lab and helps to lead several experiments and manages your lab's data server. Objectively, a single poor mark is not a major issue, but the student is taking the grade personally.

2.3. Inject #1

You meet with the student in your office. As you try to understand what is going on, it becomes clear that the student is angry about their grade, and blames you personally.

Based on the information introduced in Inject #1, discuss potential issues and key concepts that arise from this Inject. Then, identify additional decisions, communication flows, questions, and/or resources that would need to be addressed. The questions below are provided to help guide the discussion around general key points. However, these questions are not intended to define a rigid list of concerns that need to be addressed, nor will all of them be applicable to your individual situation.

1 How would you respond to the student's concerns? What tools do you have personally to try and deescalate the situation? What tools do you have to differentiate the level of risk of the student?

2 What resources are available to the student at your institution that you could provide to them? Who could you call to provide you assistance with the student in this situation?

3 Who should you contact, if anyone, within your group, department, institution, etc. to bring this situation to their attention? Is there any coordination that they would expect from you?

4 Do you have any obligations to report the students conduct or behavior to your institution by law or policy? If so, who would you need to contact?

2.4. Inject #2

Despite your best efforts, the graduate student is still very upset and decides to not sit for any other exams for the semester. As the semester draws to a close, you no longer see the student anymore in your lab. You find out that due to the poor marks, the student is being removed from their academic program. You hear that the student intends to leave at the end of the week to go back to their home country to avoid visa issues.

Based on the information introduced in Inject #2, discuss potential issues and key concepts that arise from this Inject. Then, identify additional decisions, communication flows, questions, and/or resources that would need to be addressed. The questions below are provided to help guide the discussion around general key points. However, these questions are not intended to define a rigid list of concerns that need to be addressed, nor will all of them be applicable to your individual situation.

1 What information should you gather from the outgoing student? Do you need, or want, to conduct an exit interview to better understand and learn from the situation?

2 What documentation, if any, of the work the student was conducting in the lab would be helpful to have for continuity purposes?

3 Do you have any obligations or need to allow the student to continue to access the lab after they leave? If so, what actions need to be taken to retain that access?

4 Who should you contact, if anyone, within your group, department, institution, etc. to bring this situation to their attention? Is there any coordination that they would expect from you?

2.5. Inject #3

If in Inject #2 you revoked the graduate students' access to the data server, you may skip this section. The now former student flies out on a Sunday back to their home country. The next morning, you receive several frantic emails from members of the lab. No one can access the data server for the lab, upon inspection the data server has been wiped.

Based on the information introduced in Inject #3, discuss potential issues and key concepts that arise from this Inject. Then, identify additional decisions, communication flows, questions, and/or resources that would need to be addressed. The questions below are provided to help guide the discussion around general key points. However, these questions are not intended to define a rigid list of concerns that need to be addressed, nor will all of them be applicable to your individual situation.

1 What options do you have to recover the data? How long might this recovery take (such as time to get the data to you, time to reformat the server, etc.)? How expensive would the recovery be (such as shipping a drive, AWS Egress, etc.)? Who would you need to reach out to for assistance with data recovery?

2 What research are you able to conduct without the data server?

3 Do you have any obligations to report this event to funding agencies and/or co-PI's? If so, who do you need to reach out to and by what means?

4 Do you have any obligations to report this event to law enforcement and/or Information Security Office (ISO)? If so, who do you need to reach out to and by what means? Will you be able to immediately begin rebuilding or will they need to have access to your devices for investigative purposes (such as forensic analysis)?

5 Who should you contact, if anyone, within your group, department, institution, etc. to bring this situation to their attention? Is there any coordination that they would expect from you?

2.6. Inject #4

If in Inject #2 you revoked the graduate student's access to the backup solution, or if you do not currently have a backup solution, you may skip this section. In a frantic search, you go to check your file backup solution. However, you find that the backups have been wiped and you are unable to access any of the files. It appears that your former student destroyed the copies on your backup solution at the same time as the original copy in the lab.

Based on the information introduced in Inject #4, discuss potential issues and key concepts that arise from this Inject. Then, identify additional decisions, communication flows, questions, and/or resources that would need to be addressed. The questions below are provided to help guide the discussion around general key points. However, these questions are not intended to define a rigid list of concerns that need to be addressed, nor will all of them be applicable to your individual situation.

1 Do you have additional data recovery options? Were copies kept in a snapshot system (such as file system based snapshots, snapshots managed by a third party, etc.) that could be leveraged to recover the data? If so, how long will the snapshots be preserved for you to leverage?

2 Is it possible to recover some or all of your data from an immutable source, such as a CD/DVD or Tape? Would a research partner have a copy of some or all of your research data?

3 Do you have any obligations to report this event to funding agencies and/or co-PI's? If so, who do you need to reach out to and by what means?

4 Do you have any obligations to report this event to law enforcement and/or Information Security Office (ISO)? If so, who do you need to reach out to and by what means? Will you be able to immediately begin rebuilding or will they need to have access to your devices for investigative purposes (such as forensic analysis)?

5 Who should you contact, if anyone, within your group, department, institution, etc. to bring this situation to their attention? Is there any coordination that they would expect from you?

2.7. Inject #5

If in Inject #2 you revoked the graduate student's access to your computing systems, you may skip this section. Ha ving now discovered that all of the data is gone, you try to determine if any local copies of data might have been kept on the desktops in the lab. As you begin to do this, you realize that each of the desktops have been wiped. This is when you remember that you provided your former student with access to the desktop administrative accounts in order to mount the lab file server. You have now lost all of your data and all of the custom configurations that were required to conduct your research.

Based on the information introduced in Inject #5, discuss potential issues and key concepts that arise from this Inject. Then, identify additional decisions, communication flows, questions, and/or resources that would need to be addressed. The questions below are provided to help guide the discussion around general key points. However, these questions are not intended to define a rigid list of concerns that need to be addressed, nor will all of them be applicable to your individual situation.

1 What research are you able to conduct without the computing systems in your lab?

2 Do any provisioning scripts exist to reinstall the systems? If so, how long will the provisioning take?

3 Are there resources within your group, department, institution, etc. that could be leveraged to assist in rebuilding (such as a central IT group)? If so, who would you need to contact and what cost in charge-backs, if any, would be levied?

4 Do you have any obligations to report this event to funding agencies and/or co-PI's? If so, who do you need to reach out to and by what means?

5 Do you have any obligations to report this event to law enforcement and/or Information Security Office (ISO)? If so, who do you need to reach out to and by what means? Will you be able to immediately begin rebuilding or will they need to have access to your devices for investigative purposes (such as forensic analysis)?

6 Who should you contact, if anyone, within your group, department, institution, etc. to bring this situation to their attention? Is there any coordination that they would expect from you?

2.8. Hot Wash

Questions to Consider

- Based on your discussions, what *should* happen in a best case scenario?
- Based on your discussions, what *would* happen if this event took place tomorrow?
- Having both of these discussions in mind, what *difference* exists between your current preparedness level and the best case preparedness level?
- Having completed the exercise, what went well that you would *continue* in the future? In what areas were you *unprepared?* What would you *stop* doing to improve your outcome? What can you *start* doing today to improve your outcome in a future exercise or real event?
- If you *did not* have a plan for this situation, what are your action items and timeline to create one? If you *did* have a plan, what are your action items and timeline to update it?
- When will we conduct this exercise *again?*

Participant Feedback: