The Tabletop Exercise:

Lessons Learned

Allan Alford, CISO/CTO @ TrustMAPP

Host of The Cyber Ranch Podcast

(With help from a good friend and Boston healthcare CISO)

There is never just one "The Tabletop Exercise"

- Any given exercise must be comprehensive enough to include individual contributors, management, and members of the Board.
- This means multiple sub-exercises.
- Follow-up exercises must be conducted.
- Every time.

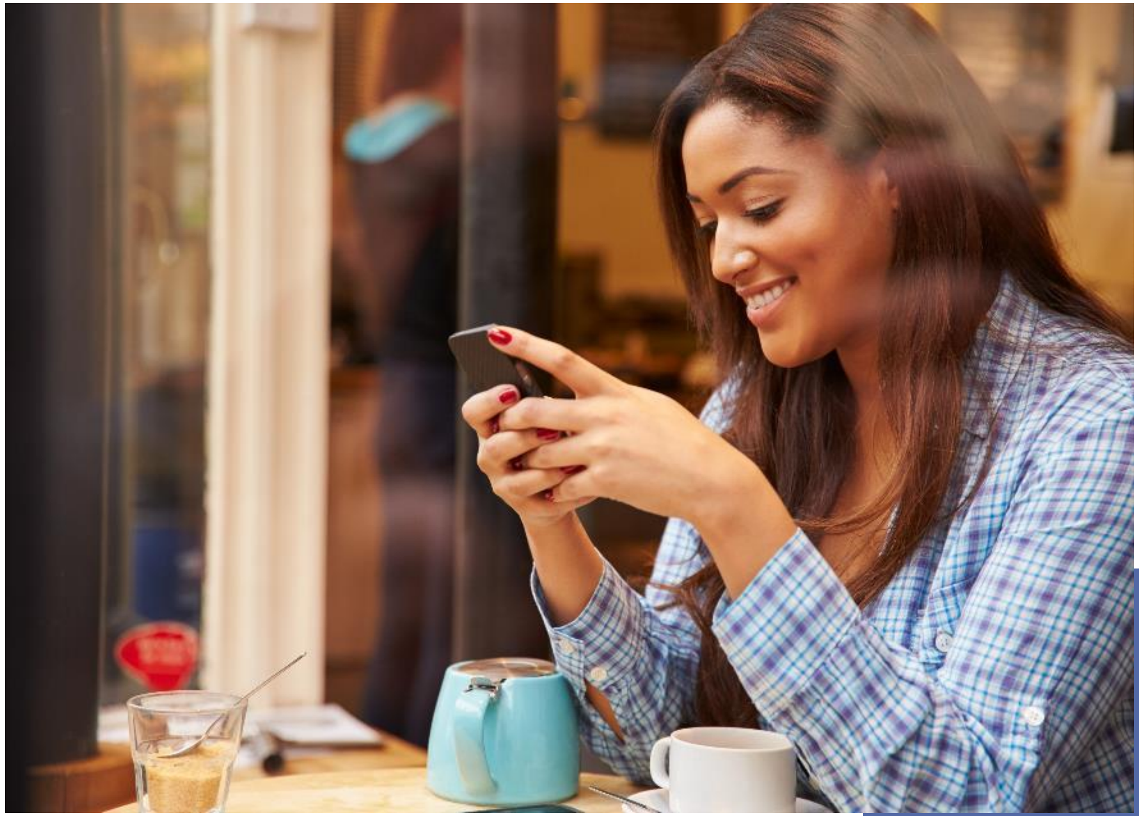
Pre-Exercise Planning

Your TTX Planner & Content Developer should be experienced.

It is SO easy to lose your audience…

If not, start here:

https://www.cisa.gov/cybersecurity-training-exercises



Measurement Is Critical

DO

- Pick only TTXs for which you can measure the impact on your organization.
- Establish measurements of impact you'll use to rate the impact of the scenario and the residual risks and impacts that event will have on your organization.
- Shoot for quantitative measurements, using your organization's existing risk measurement tooling (5x5, heatmaps, FAIR, etc.)

DON'T

- Do not pick TTXs that would absolutely obliterate your organization. The goal is to stress the organization, not destroy it.
- How do you measure that anyway?

Time & Roles

Time to commit

- Double what you think. No, seriously.
- Planner & Content Author work MONTHS in advance with “friendlies” – small dry runs.
- A comprehensive exercise can take up to 4 full days for a medium-sized organization.
- NOTE: Exercises as small as 4 hours have been successful, and ANY exercise contributes to readiness.

Roles

Participant

IR & IT teams…

Leadership…

The Board…

Facilitator

Might be you, but outsiders will be more listened to.

And professional facilitators… facilitate better.

High EQ required.

Evaluator

(Facilitator?)

Judges the event, produces the After-Action Report (AAR).

(Scribe?)

Observer

(Optional)

Non-experts whose focus is solely on organizational efficacy and teamwork.

If your facilitator is not a SME on the details of the scenario…

Ideally you have "Actors" for each "What if?" and "Now what?" who are subject matter experts.

Present the facts only – not the actual questions.

Why These Roles?

Expertise!

- Security leaders should ideally be participants and not facilitators. Again, outside expertise is often more respected, and you are probably not a trained facilitator either…
- Hire someone (preferably someone with known facilitation skills and a high EQ). If facilitator-only, support them with the facts for their “What if?” and “Now what?” questions – via actors or via your own stepping in (facts of the scenario only!!!)
- PREP YOUR FACILITATOR but be prepared to provide detailed answers to questions that will arise during the scenario.

Free or Affordable Facilitators

- Key vendors already in place doing IR/BC/DR support? Ask them to facilitate.
- Look at your insurance carriers or brokers first - they typically give these away for free.

- Have an MSSP? They have a shared fate with you - the more successful you are, the more they are. Use this to your advantage to get low- or no-cost TTX to start.

Be Prepared

BCP & IR Playbook

- Don’t drill until you have at least a rudimentary BCP and IRP in place, which means you have also performed your Business Impact Analysis assessments (BIAs) beforehand as well…

- Roles defined
- At least a rudimentary playbook for both one regional and one comprehensive disaster scenario
- Contact information and calling trees

Pre-Flight Checklist

- ALL materials related to the BCP/IRP are stored safely in MULTIPLE OFFSITE locations

- Purchase reems of pens and paper, whiteboard markers and sticky notes. Remember: at least some computers are often offline during the exercise.

- But plan on a videoconferencing solution that involves participants communicating from their various remote locations. Drills that are phone-only are also recommended.

It’s Not Just You Who Prepares

- Set a strong agenda and share it out well in advance!
- Everyone involved in the exercise should read the BCP/IRP beforehand at a minimum. If participants outside of the BC/DR teams recognize the scope and depth of planning, they will have a deeper appreciation of the exercise. (It also helps them react).
- Warn them of time commitments…

- What is a TTX? Explain that thoroughly up-front, emphasizing a no-fault, no-blame environment.
- Surprises suck. Minimize their usage.
- Pre-work should be relevant to your audience. Remember the Three O’s:
    - Outages
    - Objectives
    - Outcomes

During the Exercise

The goal is to strengthen your organization. Period.

Fault and blame have no place here.

Humans Are, Well… Human

Emotions

- These exercises are exciting and stressful. They will affect every participant differently.
- Be sure to recognize the feelings in the room as you proceed from step to step and phase to phase. Acknowledge the stress/pain/fun/sadness you experience as your organization uncovers its problems.

Teamwork Makes the TTX Work

- Encourage each other. Commit to partner on fixing challenges - no single problem is a single person's issue.
- While single threaded ownership may be required to bring an issue to closure, fixing anything hard is very rarely the result of one person's effort - remember, TTX is a team sport!

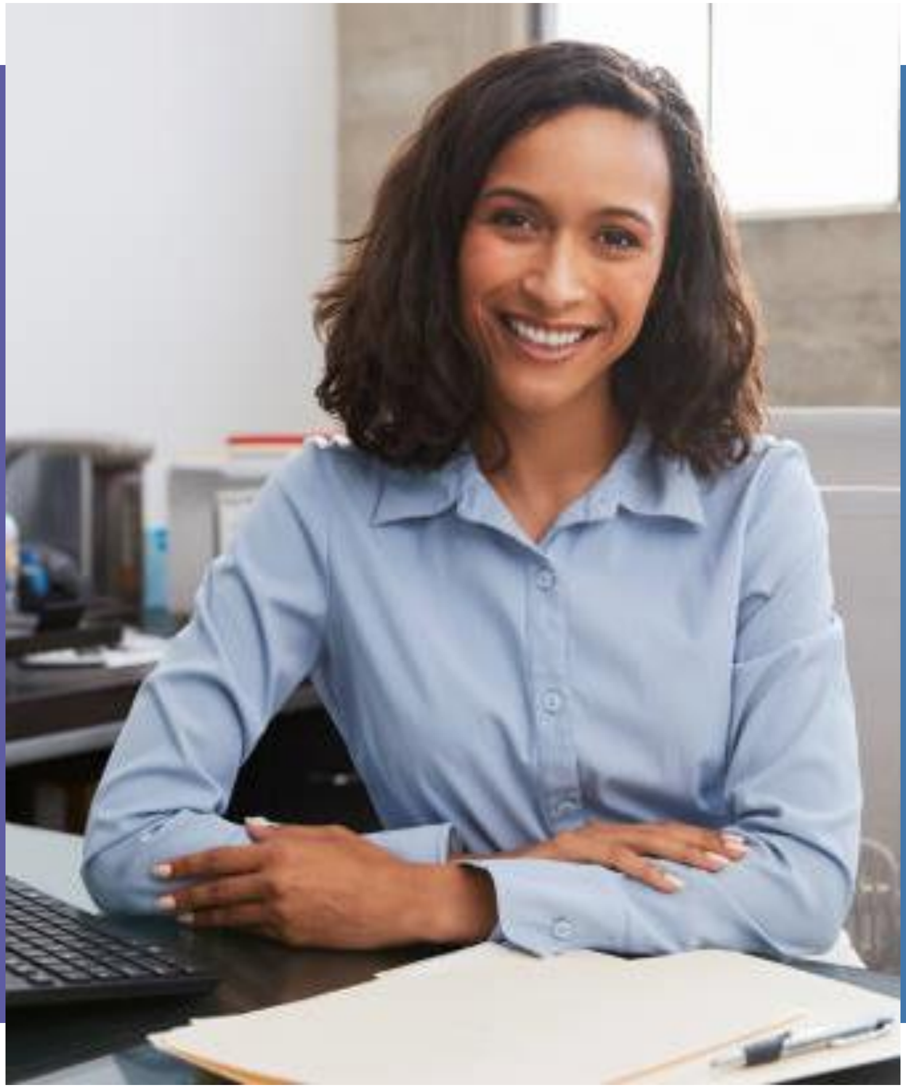
More About Your Audience, Part 1

- Executive leadership/Board:
- Low complexity TTXs work best and those that require Board decision making and communication play well here.

- Company management:
- Moderate complexity (and moderate difficulty) TTX meant to exercise the incident response mechanisms, including PR, communications, marketing, physical security, facilities, IT, business operations, and other.

More About Your Audience, Part 2

- Incident responsetTeams:
- High complexity and difficulty TTXs - these are meant to stress the team and validate IR plans, playbooks, and tools to discover, assess impact, take action, and recover operations.
- These are typically done with individual incident response teams with scenarios relevant to their day-to-day.



- You don’t always need a proper TTX for these:
- Get creative - Purple Teams are an excellent ‘Table Top’ exercise and something you should perform regularly anyway.

“What if?”, “Now What?”, But “No Surprises”? (Stress Appetite)

Your deal with the organization is to strengthen their resiliency, not to bully them.

Finding out that resources they have always relied upon are not available during the scenario improves their planning.

The occasional surprise is okay; just don’t drop BIG bombs on them or bombard them with too many small ones. “That is also offline” should be used sparingly.

The goal is to give everyone a better action plan and muscle memory for when a real scenario occurs.

Track Outcomes Real-Time If You Can

Observations

- Every observation requires capture and most require a response/remediation action be captured real-time as well – especially if the area emphasized is beyond your stress appetite.

Outcomes

- Rate outcome severity/impact using the organization’s existing risk measurement & prioritization method.
- Don't make up your own model to speak to outcomes – use the organization’s existing model.

Post-Exercise Follow-Up

Brag!!!

- Showcase that the exercise was a success in that it uncovered new areas of risk.
- The exercise also trained the organization with some new “muscle memory”. Preparedness is most definitely enhanced.
- Everyone learned something. Capture those learnings and share them out.

- The team themselves are probably exhausted, but they probably also earned that.
- Praise the participants - Especially those who are not part of the BC/DR organization or IR teams!
- Be prepared to speak to specific measurement of all outcomes – not just findings. You did measure, right?

Post Mortem – What You Measured - AAR

Team Performance

- The Facilitator, Evaluator or Observer can speak to specific moments of teamwork, or its absence.
- Communication hiccups can be discussed here – even ones due to technical factors.
- Judgement of the stress appetite should be included here as well – how well did YOU do in creating a viable, realistic scenario that tested the organization without just punishing it?

Organizational Readiness

- Quantify the risks uncovered.
- Speak to specific gaps in readiness without judgement.
- Share those tracked outcomes!
- If you cannot produce the full plans to address in a timely manner, state that such plans are immediately coming to address a highly specific list of outcomes. Give yourself an aggressive deadline let you lose momentum!

May All Your TTXs Be Winners!