



# Tabletop Exercises

How to Successfully Run Incident Response Tabletop Exercises

Barry Suskind

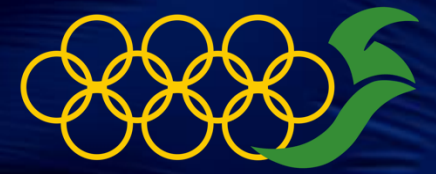
Senior Director (retired) Threat Detection & Response, Cybersecurity



# Intro/agenda

- Who am I and what do I know?
- Agenda





# Tabletop Exercises

- What are they?
- How do they compare to disaster/recovery drills?
- What purpose do they serve?



# Technical Tabletop Exercises

- Understanding gaps in your enterprise
- Fully exercising cyber security teams
- Having non-cyber technical folks to think more about security
- Learning and putting into practice following procedures
- Teach how to contain information flow





# Business Tabletop Exercises

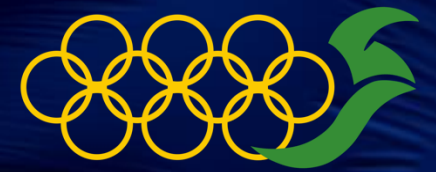
- Engage executive staff in difficult situations
- Understanding the incident response process
- Preparedness for when bad things happen, and they do
- know when to make difficult decisions
- With executives and the board, messaging is key



# Combined Tabletop Exercises

- Having both technical, business and executives in one exercise
- Longer meeting times
- Exposes all teams to the complete picture
- Many Challenges





# Pre-Planning the Exercise

- What type of exercise?
- How much time should a tabletop exercise take?
- Ensuring incident response plans are current
  - Current list of key personnel and contact information
  - Has technology made aspects of the plan obsolete?
- Scheduling
  - Knowing vacation and operational schedules

# Details of an Exercise

- Defining a scenario

- What aspects of your enterprise will be the target?
- Understanding the Enterprise and the People
- Keeping current on industry-wide issues and breaches

- Break the scenario into pieces called "injects"

- Each inject reveals a bit more information of the "breach"

- Understand timelines
- Don't skip steps

Sample 1 Sample 1

**What is state of the world?** After researching software on application servers used in the new network, it is found that use of Apache external IP address is prevalent across the enterprise.

However, it is found that 15 of the 100

**What is state of the world?** Apache users are using a applications version from 2012 and have never backgrounded updates. In fact, user contacts addresses are not being kept longer open though OneDrive installation was not after asking for vulnerabilities are discovered.

**What is state of the world?** and Sharepoint configuration, it shows that operations team is not up to date with Open Source recovery plan. **What is state of the world?**

**What is state of the world?** multiple users contact helpdesk saying they cannot open word documents on their PC's or they open with gibberish.



# Lets Talk About Scenarios

## Session Hijacking

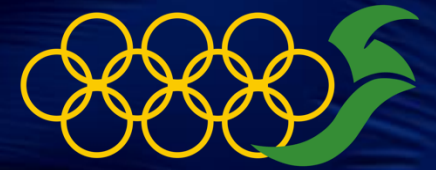
- I've created many encryption difficult
  - AitM via phishing
- I've helped others to make it more plausible
  - BitM via browser takeover
  - Microsoft 365
- Frustrations when I was only a participant
  - AitM-Auth in the middle
  - BitM browser in the middle
- Common take away when 3<sup>rd</sup> party runs your tabletop
  - Assume cloud protects
  - Executive preparedness
  - Lack of MFA
- Consider excluding key email outage
  - Service accounts and syncing
  - Linux CUPS vulnerability
- Some examples, just from reading the news
  - External party claims to have data provided by a current employee
  - Unix/Linux printing service
  - RCE, but only maybe
- When speaking with staff about how things work, be careful



# Running the tabletop

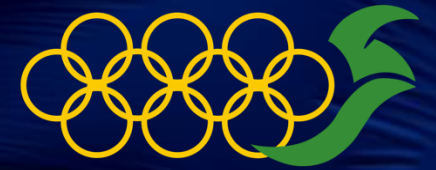
- Introduction
- The exercise
- Close out
- Next steps





# After the tabletop

- Prepare action report
  - Detail the exercise
  - Highlight the gaps
- Create executive summary
  - Make sure this has a positive spin
- Assign corrective actions to appropriate teams
  - Want actions to be done in a timely fashion



# Pitfalls Of Tabletop Exercises

- Challenges with using outsourced incident response vendors
- Scheduling
- Disbelievers
- Lack of attendance
- Lack of engagement during exercise
- Difficulties in completing corrective actions





# It's a wrap

- Types of Tabletop Exercises
- Primary Elements of the exercise
- How to run the exercise and handle questions
- Dealing with the results and outcomes
- Working with third parties to facilitate your Tabletop Exercise