Welcome

Incident Response, Communications Plans, and Tabletop Exercises, Oh My!

Brad E. Rhodes

RMISC 2024

“Preparation is everything.”

- David Robinson

1 Welcome

2 WHOIS: Brad Rhodes

3 Presentation Roadmap

4 Incident Response (IR) Plans

5 Communications Plans

6 Table Top Exercises

7 Summary

8 Questions & Answers & Discussions

accenture

Accenture Federal Services

WHOIS: Brad Rhodes

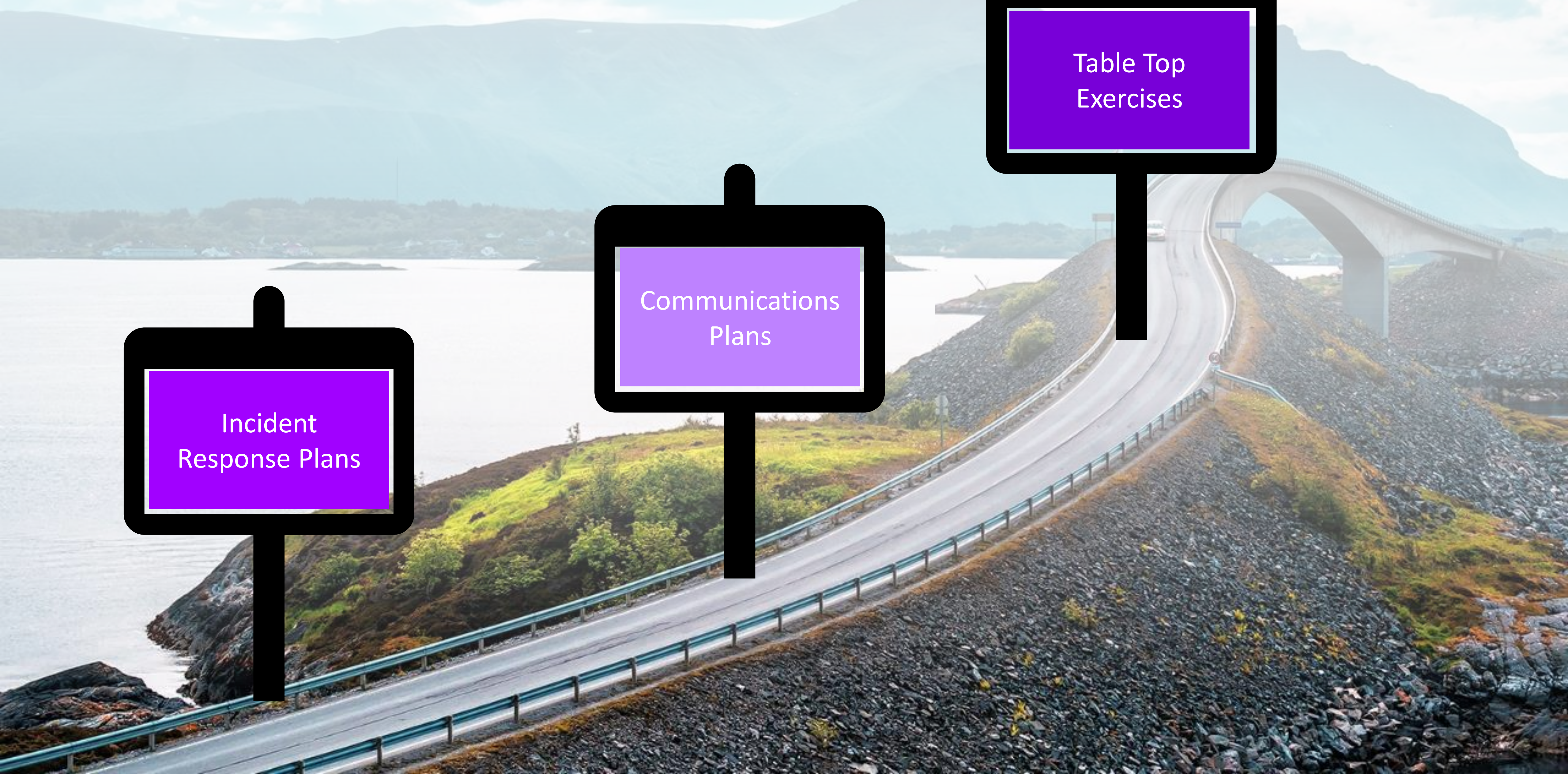
TLDR:

- **Senior Manager, Accenture Federal Services**
- COL, Cyber (17A), 63rd Readiness Division, G6/CIO
- Military Cyber Professionals Association, HammerCon Co-Lead, CO Chapter President
- Speaker, Author, Professor, Coach
- #toomany Pro-Certs, highlights: CISSP-ISSEP, CISM, CDPSE, PMP, CEH, GMON, GCIH, Cloud+, CySA+
- Extra Class Amateur Radio (HAM): KG4COS

Feel free to view/listen/grab my previous presentation/articles here: https://github.com/cyberguy514

Credit: © & TM Owning Organizations

Presentation Roadmap



Incident Response Plans

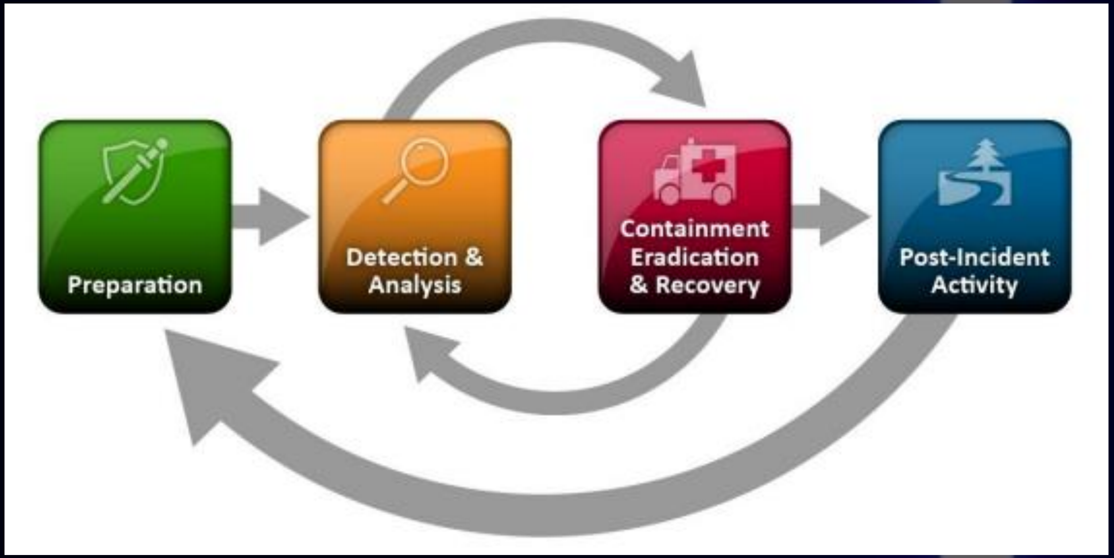
Communications Plans

Table Top Exercises

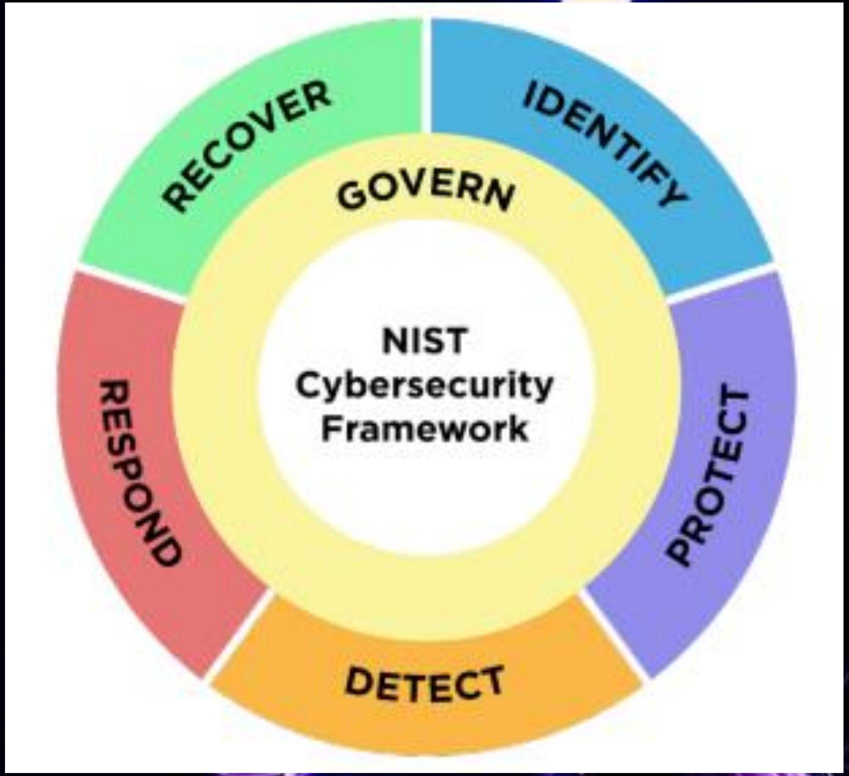
Incident Response Plans

NIST: IR Phases

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf



https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf



Cybersecurity Framework (CSF)

Expanded IR Phases

Tactical steps in IR, should be in the plan!

Preparation

People, Process, Technology, & Tooling + Planning!

Identification

Catching threat actors in your environment

Containment

Isolate threat actors and their activities

Eradication

Remove threat actors and their artifacts from the environment

Recovery

Restore systems and data to pre-incident capabilities

Lessons Learned

What should be sustained? What needs improvement?

Incident Response Plan Framework

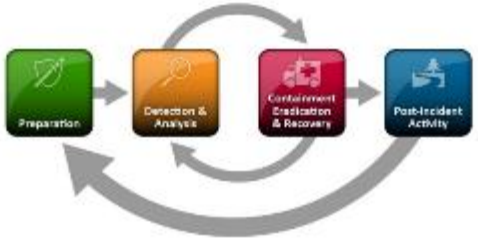
These are general guidelines that should be tailored to your organizations!

1. Identify Critical Assets/Key Terrain: prioritize **most important** assets and address those first (key server versus workstation)

2. Determine Key Stakeholders: who is responsible, accountable, consulted, and informed; who is the **incident commander**

3. Tools, Visibility, & Logs: what tools are used in IR; do we have **complete visibility and logging** or is it limited based on resources available

4. Response Actions: **timelines** based on incident severity

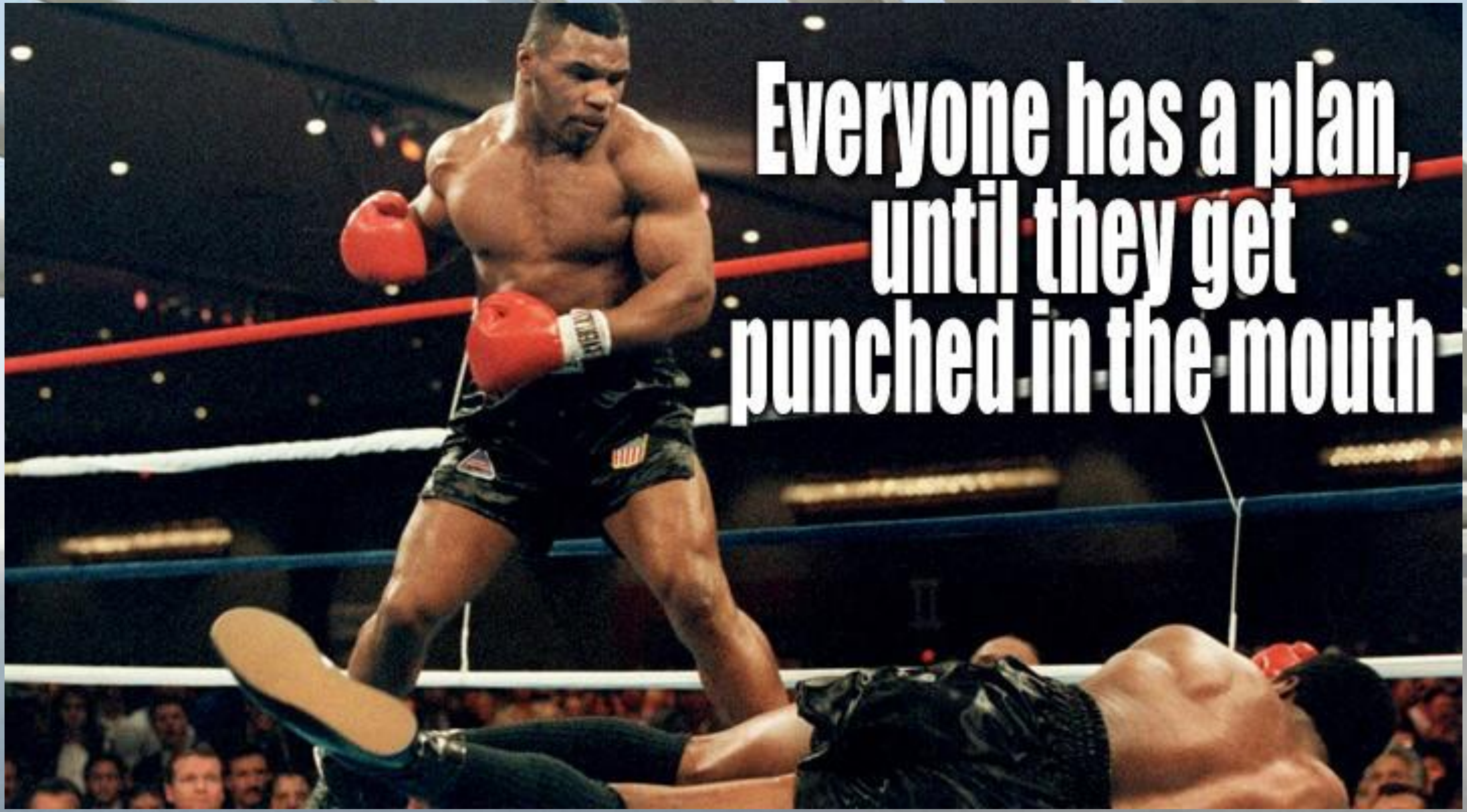


5: Communications: define **internal** and **external** comms and interactions with customers, third parties, and authorities

6. Training & Exercises: **Table Top Exercises (TTX)**; hands-on exercises (Red vs Blue); Purple Team exercises

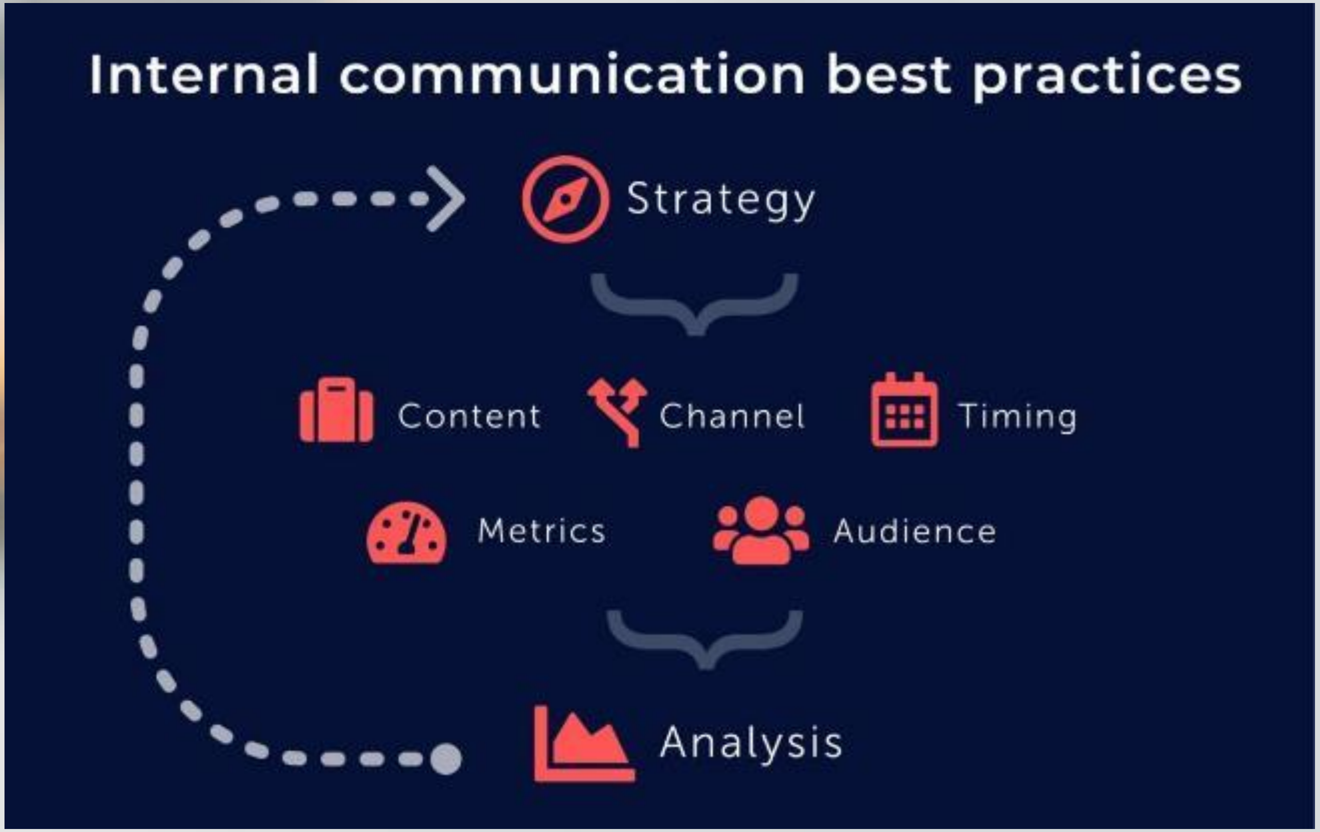
Why don’t we have IR Plans?

Why we need IR Plans?



Communications Plans

Internal Communications



Internal communication best practices

Strategy

Content

Channel

Timing

Metrics

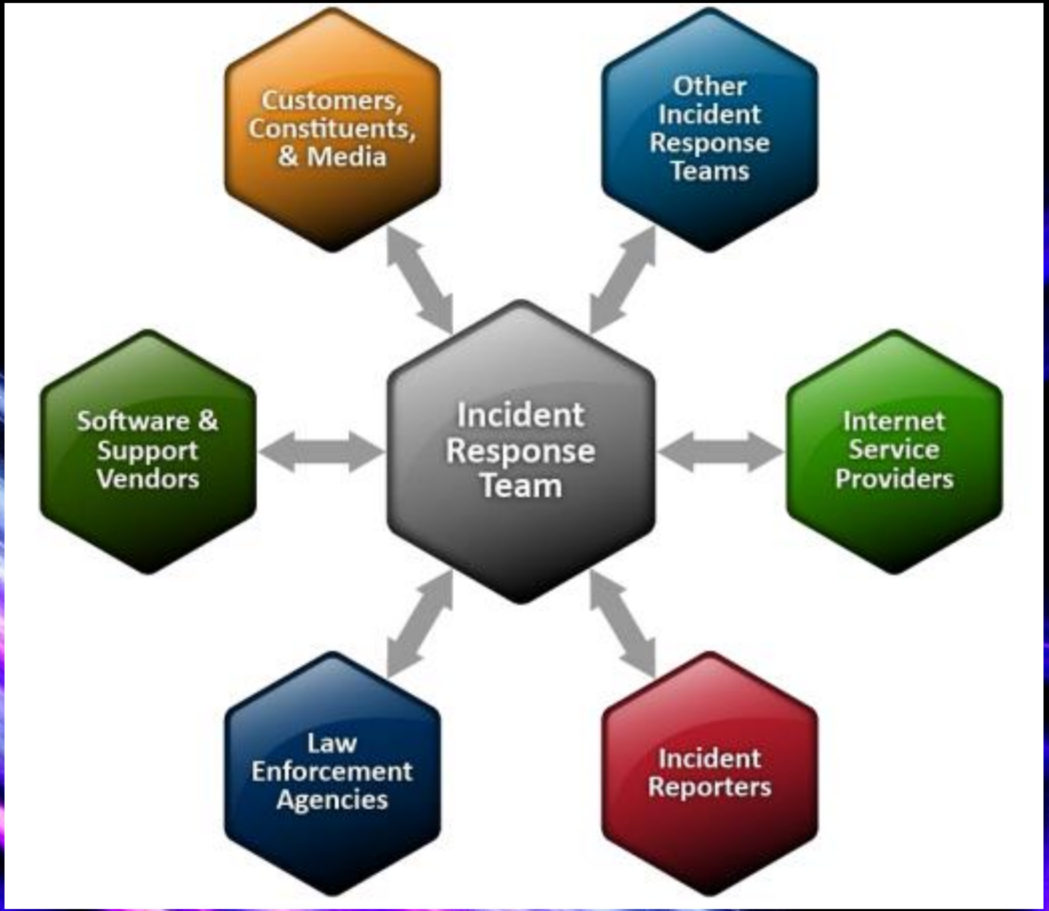
Audience

Analysis

https://intranetconnections.com/blog/internal-communication-strategy/

Key Point: Who else needs to know?!

External Communications


Customers, Constituents, & Media
Other Incident Response Teams
Software & Support Vendors
Incident Response Team
Internet Service Providers
Law Enforcement Agencies
Incident Reporters

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

https://vendorcentric.com/single-post/do-you-really-know-your-third-parties/

Communications Plan Framework

These are general guidelines that should be tailored to your organizations!

1. Communication Requirements: what needs to be communicated and when; **who needs to know?**

2. Public Affairs: who interacts with media; what is the frequency; **standardized messaging** templates

3. Customer Notifications: when and how are impacted **customers notified**; what about the information is shared

4. Third Party Coordination: did the **breach** occur at a supporting third party? do you have solid list of all assets maintained or accessed by third parties?

5: Regulatory Authorities & Law Enforcement: do regulatory bodies require **reporting**; when should law enforcement be engaged

6. Training & Exercises: practice comms **before the incident**; organization messaging during a crisis can make or break reputation

Why don’t we have Communications Plans?

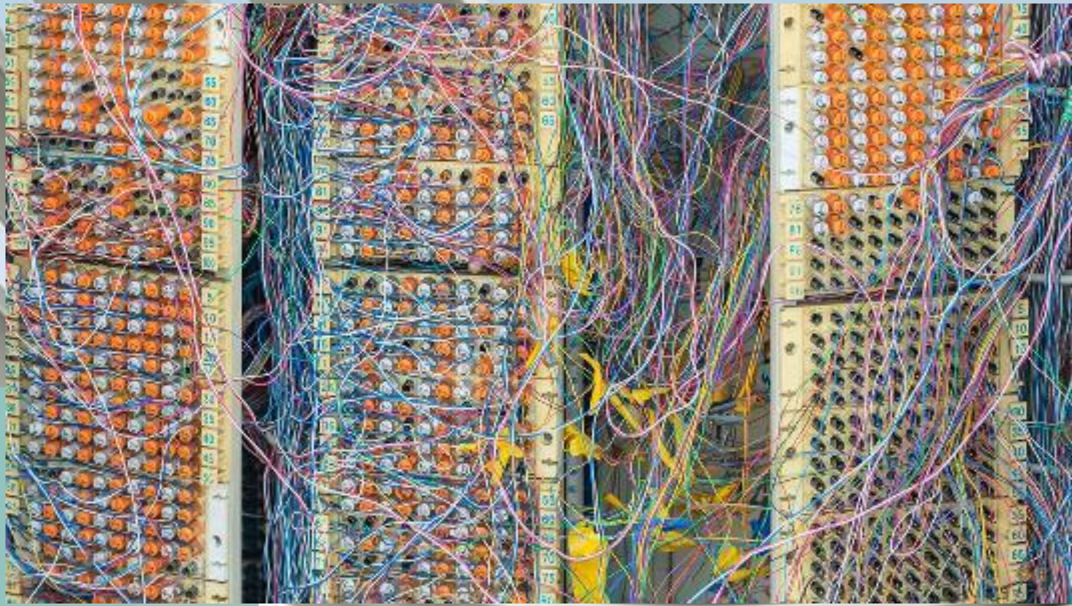


Table Top Exercises (TTX)

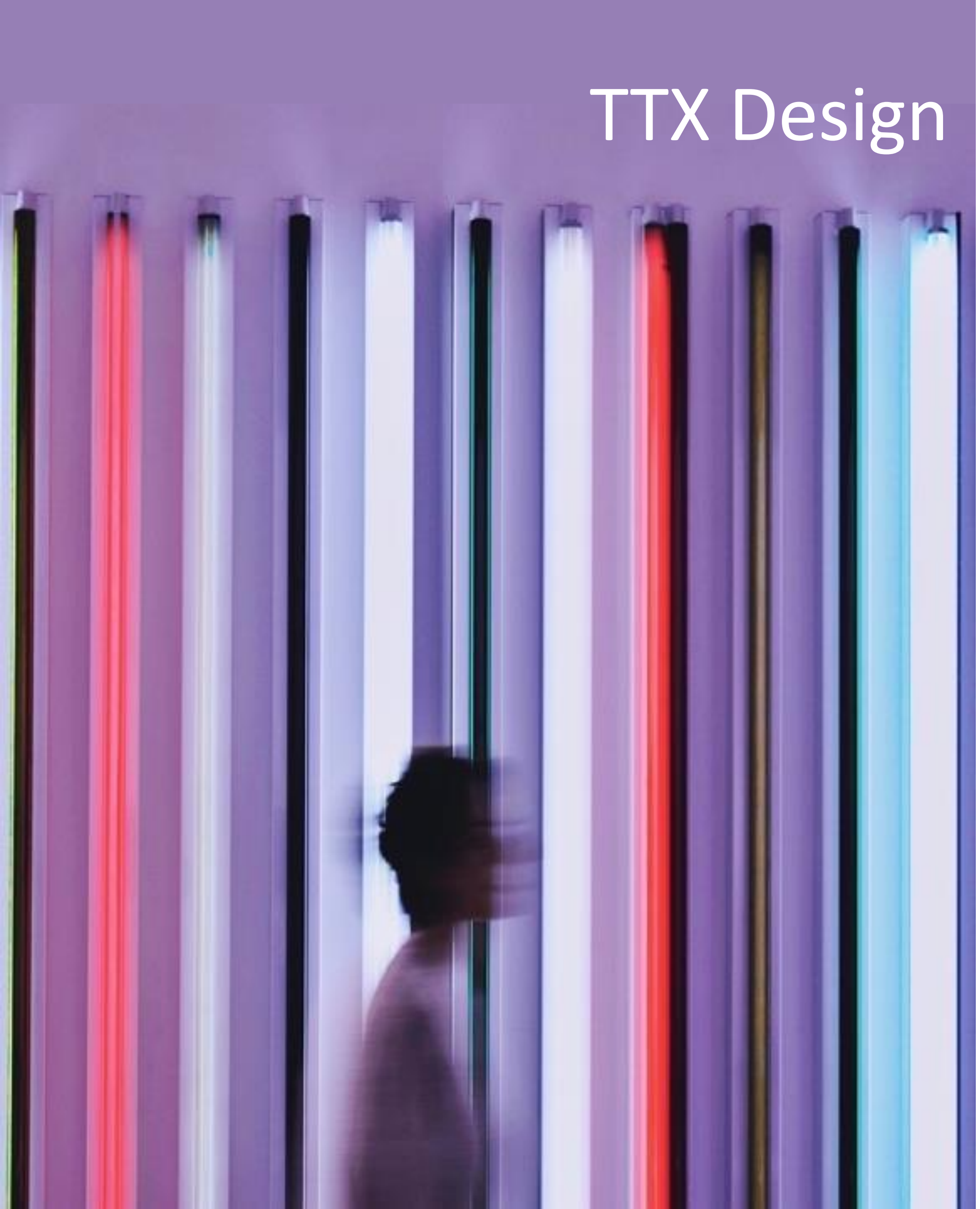
Why don’t we exercise?

IR & Comms cannot be a “pick up” game!

The Solution: TTX(s)!

What kinds of scenarios can you TTX?

- Supply Chain
- Ransomware
- Insider Threat
- Data Breach
- Social Engineering
- Cloud Security
- SCADA/OT/ICS



TTX Design

01

Objectives

02

Scenario/Story

03

Injects

04

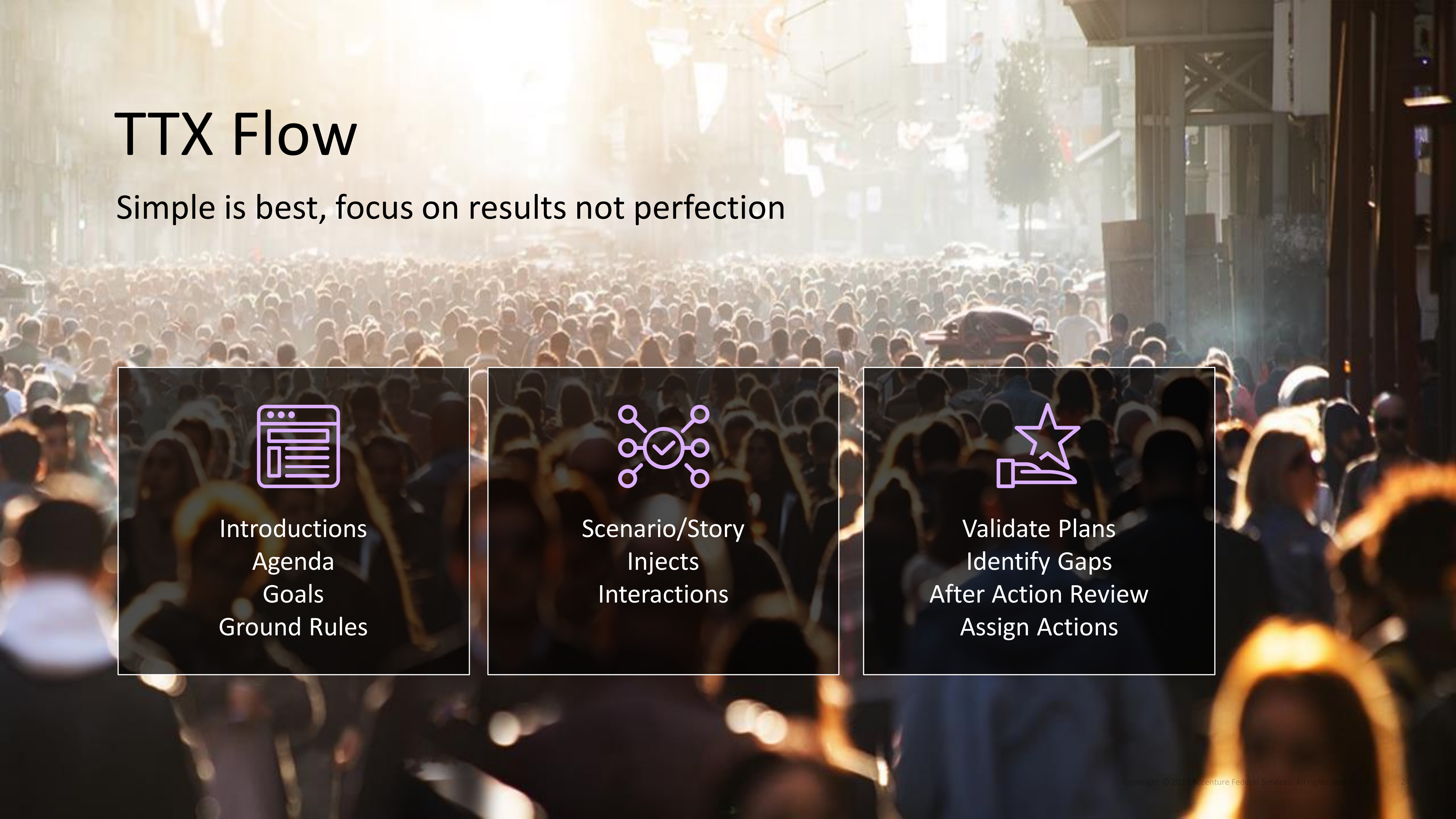
Evaluation

TTX Participants

C-Suite (CEO, CIO, CISO, CFO – key stakeholders), Cybersecurity Team(s) (SOC, CTI, Tier 2/3), Information Technology (IT) Team(s), Legal, Public Affairs, Business/Process/System Owners

TTX Flow

Simple is best, focus on results not perfection



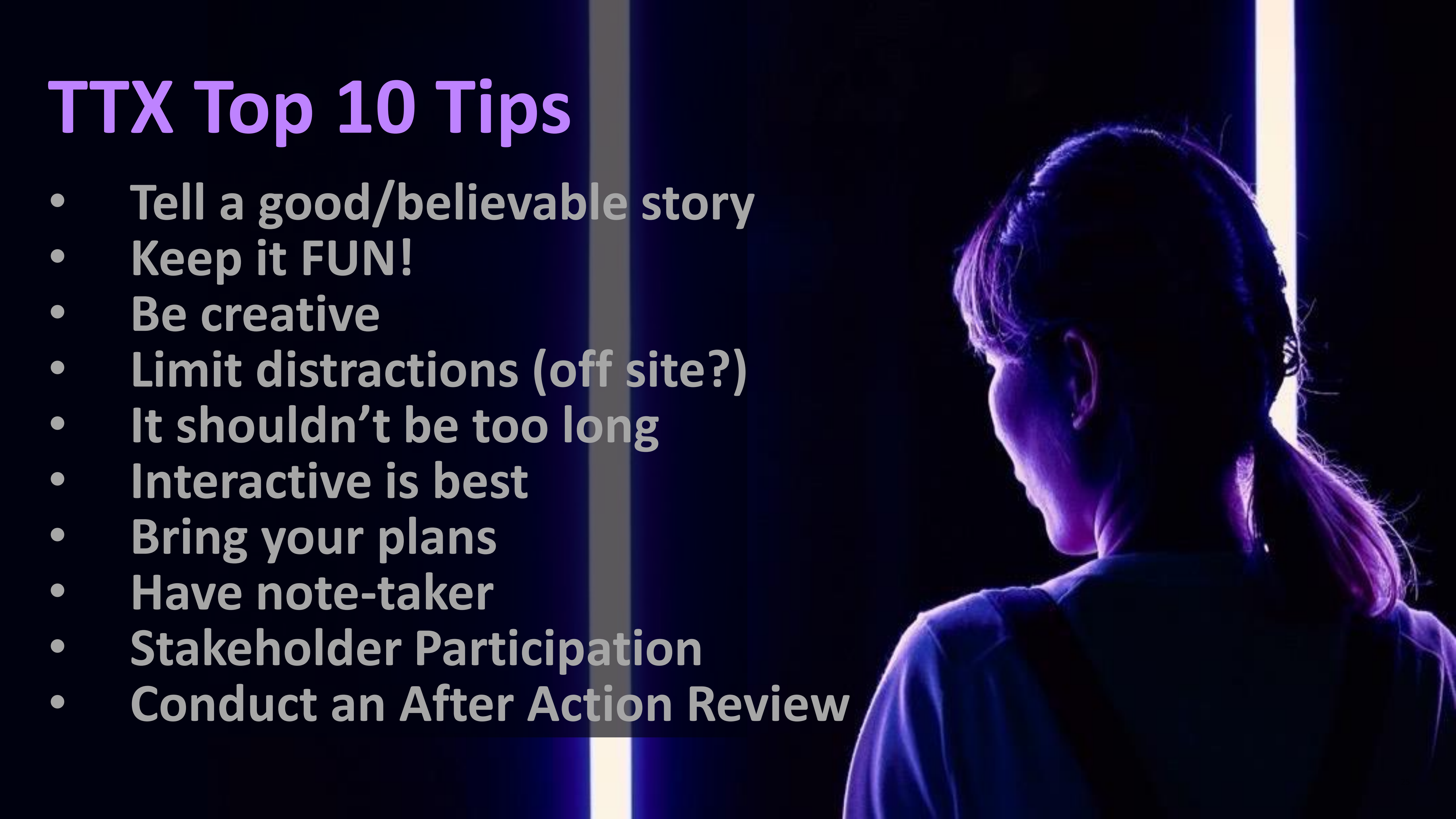
Introductions
Agenda
Goals
Ground Rules

Scenario/Story
Injects
Interactions

Validate Plans
Identify Gaps
After Action Review
Assign Actions

TTX Top 10 Tips

- Tell a good/believable story
- Keep it FUN!
- Be creative
- Limit distractions (off site?)
- It shouldn’t be too long
- Interactive is best
- Bring your plans
- Have note-taker
- Stakeholder Participation
- Conduct an After Action Review



TTX Resources

Ready.gov

https://www.ready.gov/exercises

CISA.gov

https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

CISecurity.org

https://www.cisecurity.org/insights/white-papers/six-tabletop-exercises-prepare-cybersecurity-team

FEMA.gov

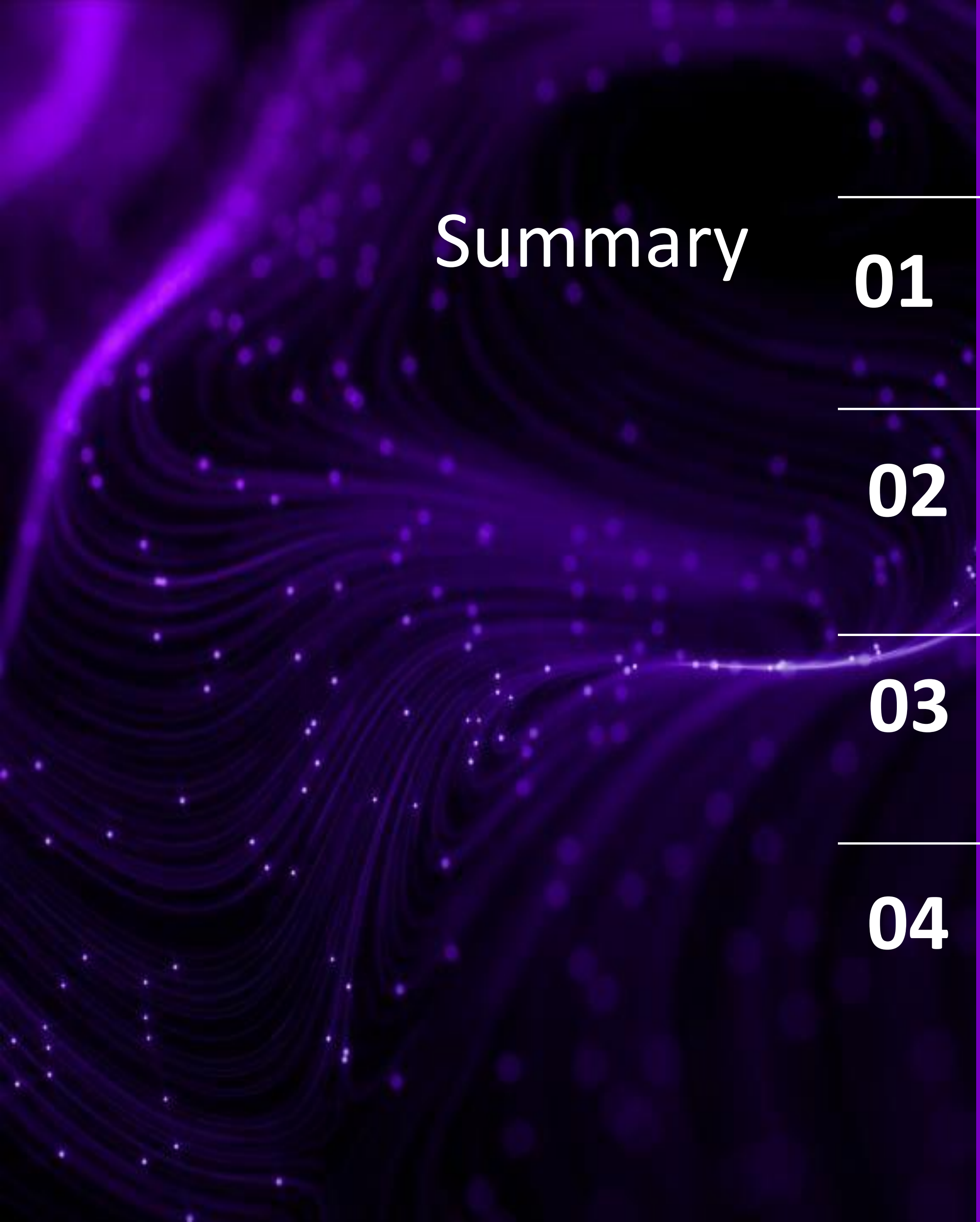
https://training.fema.gov/programs/emivttx.aspx

NARUC.org

https://pubs.naruc.org/pub/615A021F-155D-0A36-314F-0368978CC504

CriticalStart.com

https://www.criticalstart.com/tabletop-exercises/



Summary

01 **IR Plans** are key to “preparing” for the inevitable incident

02 **Communications Plans** need to be practiced – especially by senior executives interacting with the media

03 **TTXs** are the least expensive exercises that provide value and validation for plans

04 Complete IR Plans, Communications Plans, and TTX **“left of boom”**

Thank you RMISC!

Q & A & Discuss!

Happy to connect: https://www.linkedin.com/in/brad-e-rhodes-the-terminal-colonel/