RSAConference2019
San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: LAB1-T08

How to Run a Cyber-Incident Response Exercise Using an Open-Source Scenario

Tim Wiseman
Author

@cybersecex

John Elliott
Data Protection Specialist

@withoutfire

Two disclaimers

2v3

Nothing in this presentation represents the views of John's employer.

This presentation is not intended to be legal advice.

If you require legal advice you are advised to consult a qualified lawyer in your jurisdiction.

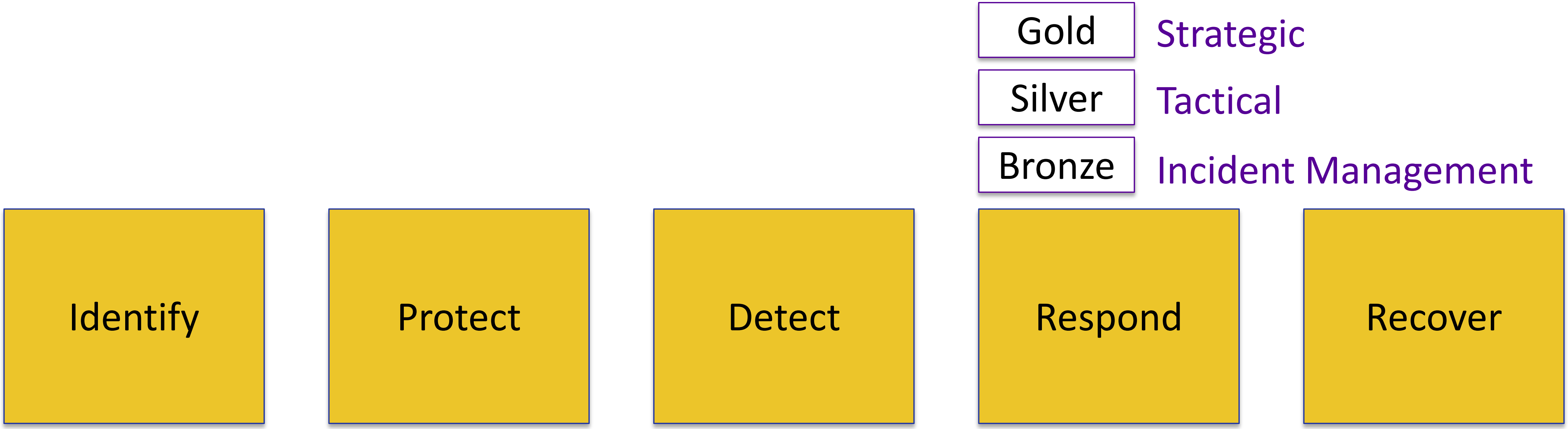
Agenda

- Why practice an incident?
- Preparation
- Facilitation
- Have a go!

Why practice?

John

NIST cyber security framework



Gold Strategic

Silver Tactical

Bronze Incident Management

Identify

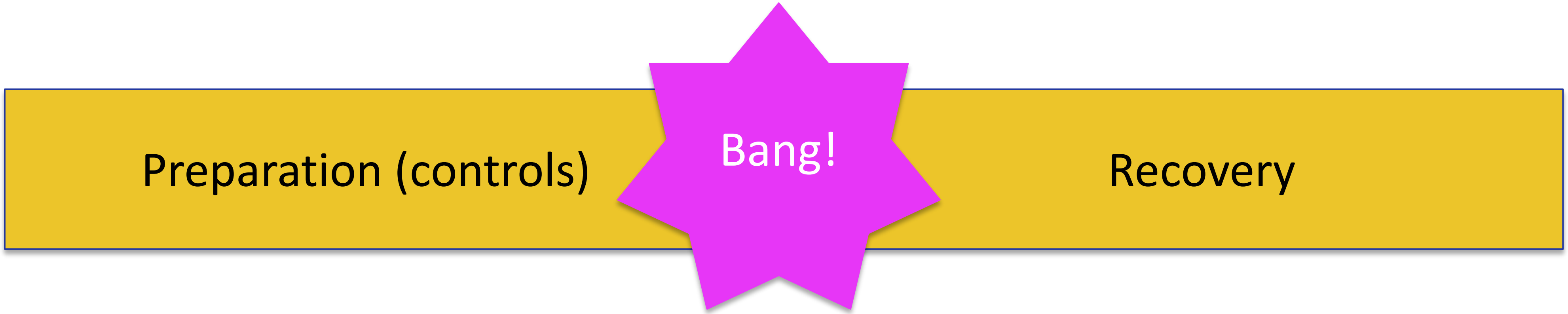
Protect

Detect

Respond

Recover

“Right of bang”

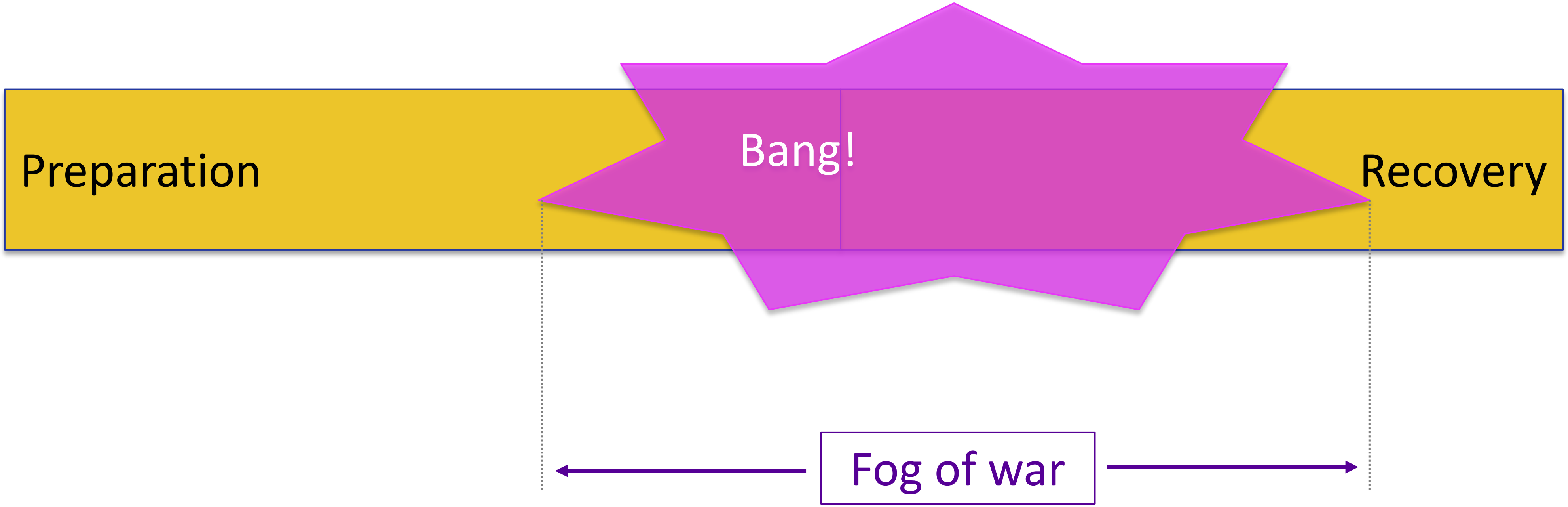


Preparation (controls)

Bang!

Recovery

There really isn’t just a bang



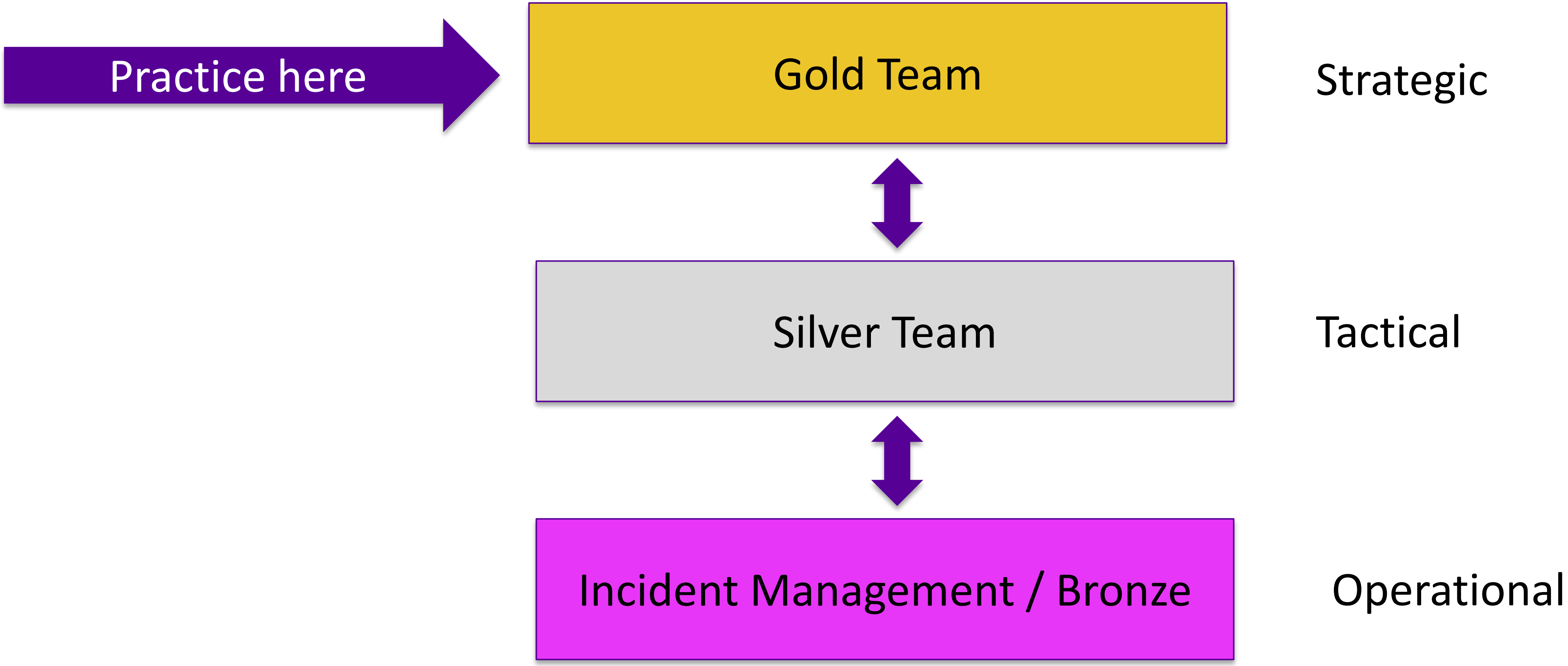
Why practice?

- Get the top team to actively think about this
  - It’s not just a theoretical playbook or an IT issue
- It’s better to make mistakes when the world isn’t watching
- We all learn from mistajes 🙂
- It’s very trite but …
- Personnel change frequently
- A control without assurance is not a control

Preparation

John

Typical incident management



Practice here

Gold Team

Strategic

Silver Team

Tactical

Incident Management / Bronze

Operational

Typical Gold Team members

- Chief Executive Officer
- Chief Operating Officer
- Chief Financial Officer
- CIO / Head of IT
- General Counsel / Head of Legal
- Heads of:
  - Marketing / PR
  - HR

Overcoming objections

We don't have time

Incidents are unknowable

It won't happen to us

We can do this without practice

It takes 2 hours. It can save a fortune.

The general principles are the same.
Mostly the questions you need to answer are the same.

You can, and historically people who do this don't do very well.

🙂

RSAConference2019

Facilitation

Tim

Facilitation: Setting the scene

1. Establish a safe place

2. Elicit expectations

3. Agree rules

4. Clarify roles

There are slides for this on the website

1. Establish a safe place

It's fine to pause, stop, think

If you feel pressured, say so

Have fun

We're <u>all</u> here to learn…

It's fine to say "I don't know"

2. Elicit expectations

What are the participants hoping they will achieve?

- Gaps in our knowledge, processes, technology
- Things we can do better
- Training our breach response safely
- And anything else?

3. Agree rules

Role play (or not)

How long?

Interruptions

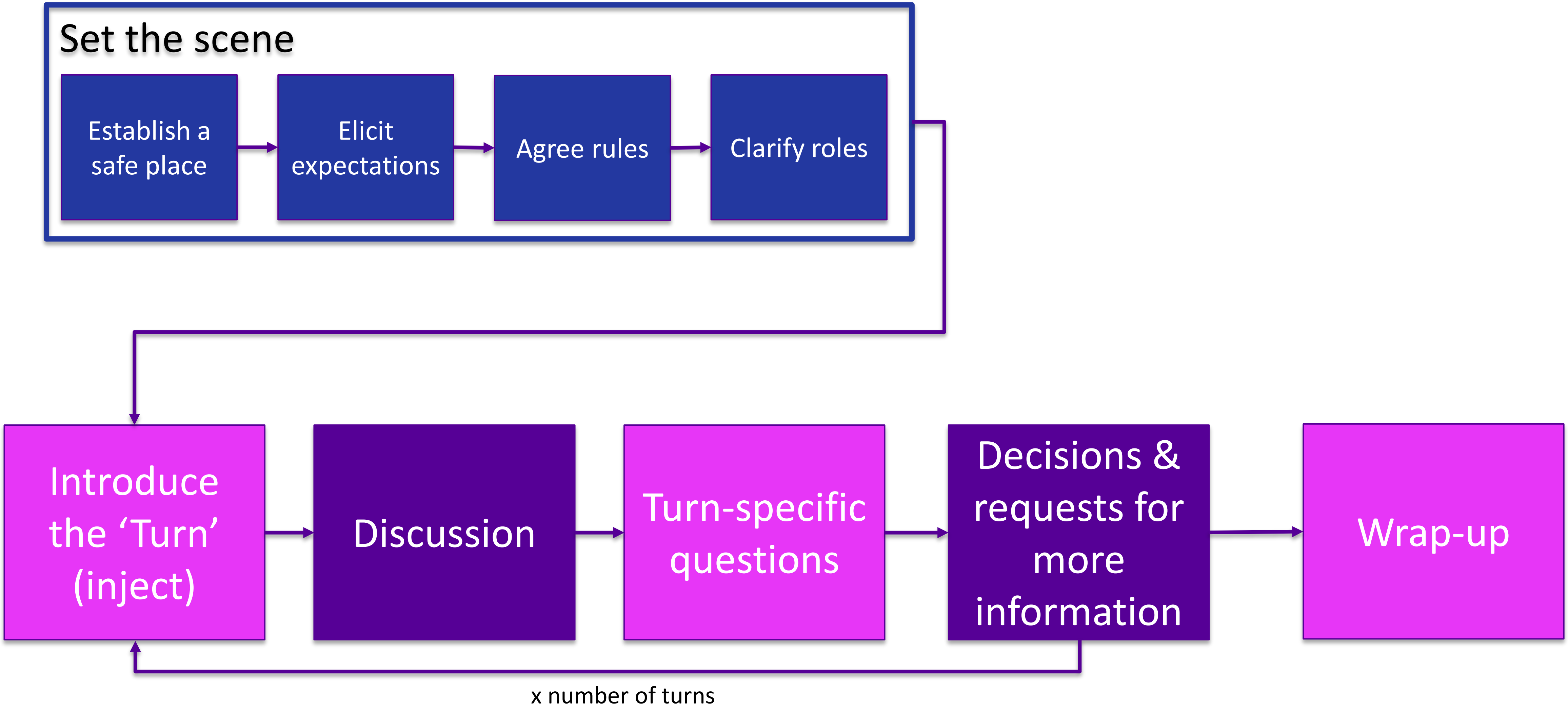
Timeouts

Car park

4. Clarify Roles

- Introductions and roles
- Gold leader
- Reserve gold leader (after *n* hours)
- Note takers
  - For the incident (they also need to practice).
    Important in real incidents for legal protection and “memory”
  - For the exercise (capture lessons)
- Someone responsible for post-exercise change

Structure of the exercise



Set the scene

Establish a safe place

Elicit expectations

Agree rules

Clarify roles

Introduce the 'Turn' (inject)

Discussion

Turn-specific questions

Decisions & requests for more information

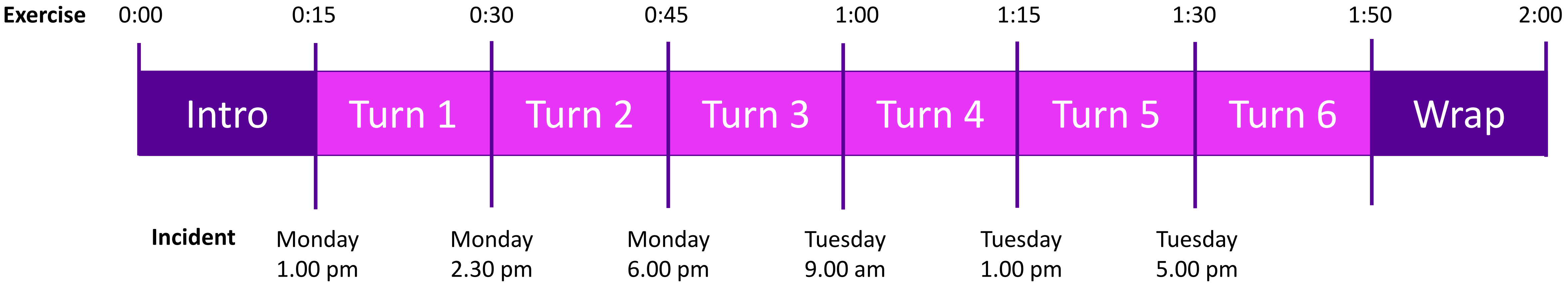
Wrap-up

x number of turns

Facilitation tips

- Know your audience
- Allow conversation, deviations, learning
- GET THE DECISIONS at each turn – bring focus to the end of the turn
- Gently keep things moving

Incident timeline



Exercise		Incident
0:00	Intro	
0:15	Turn 1	Monday 1.00 pm
0:30	Turn 2	Monday 2.30 pm
0:45	Turn 3	Monday 6.00 pm
1:00	Turn 4	Tuesday 9.00 am
1:15	Turn 5	Tuesday 1.00 pm
1:30	Turn 6	Tuesday 5.00 pm
1:50	Wrap	
2:00		

RSAConference2019

What you need

John

Free to use, open-source resources

Introduction slides

(Any scenario)

Facilitator Overview and Turns

(Scenario specific)

Turn slides

(Any scenario)

Handouts

(Scenario specific)

All can be customized to make it real for your organization.

e.g. today's exercise: <SENSITIVE_DATA> = credit card data; <CELEBRITY> = Elon Musk.

www.cybersecurityexercises.com

RSA®Conference2019

How to start an exercise

Tim

Roles for the learning lab

- Facilitator
- Chief Executive Officer
- Chief Operating Officer
- Chief Financial Officer
- Head of IT
- Head of Legal
- Head of Marketing
- Head of HR

Roles

Facilitator

- Find the pack
- Introduce turn injects
- Respond to all questions as ‘leader’ of Silver team
- Move the exercise along today
- Get the required decision

Facilitator Pack

1. Facilitator introduc (just fo
2. Role la
3. Turn ha

Start to read the facilitator introduction now!

Roles

Chief Executive Officer

- You care about:
  - Day to day activities with your COO
  - Communication to the Board

- How do we clean this up?

Chief Operating Officer

- You care about:
  - Day-to-day business operations
  - Resourcing the problem

- How do we contain and then clean this up?

Roles

Chief Financial Officer

- You care about:
  - Money
  - Effect on share price / market confidence / credit rating
  - Investor relations
- Do I get the blame for previous underinvestment?

Head of IT

- You care about:
  - IT infrastructure
  - IT Security
  - User satisfaction
- Do I get the blame for this?

Roles

Head of Legal

- You care about:
  - Legal affairs of company
  - Regulatory issues
- Does this open us up to litigation risk?

Head of Marketing

- You care about:
  - Company’s marketing campaigns
  - Company’s goals
  - Our customers
- How does this incident and our reaction affect our brand?

Roles

Head of HR

- You care about:
  - People strategy
  - Culture of organisation
- Employee relations (e.g. a strike!)
- Does this issue open us up to HR issues?

RSAConference2019

Let’s do it!

You!

RSAConference2019

Wrap-up

John

Wrap-up

- Do you feel confident you can run an exercise?
- What else would you like to have?
- If we ran this lab again, what should we change?

What next for you…

- Schedule an exercise within the next six weeks!
- Remember to customize the slides and handouts
- Talk to silver and gold team leaders to see which exercise and format will work best for your organization
- This is a journey.
  The more an organization practices, the better it gets.

RSAConference2019

Thank you

Tim @cybersecex | **John** @ withoutfire

www.cybersecurityexercises.com