

RSAC[®]Conference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN
ELEMENT

SESSION ID: LAB3-R08

HOW TO RUN A CYBER-INCIDENT RESPONSE EXERCISE USING AN OPEN- SOURCE SCENARIO



Aaron Rosenmund

Author Evangelist
Pluralsight
@ARosenmund

John Elliott

Author & Consultant
Pluralsight & others
@withoutfire

#RSAC

Two disclaimers

1v2

Nothing in this presentation represents the views of John or Aaron's employers.

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

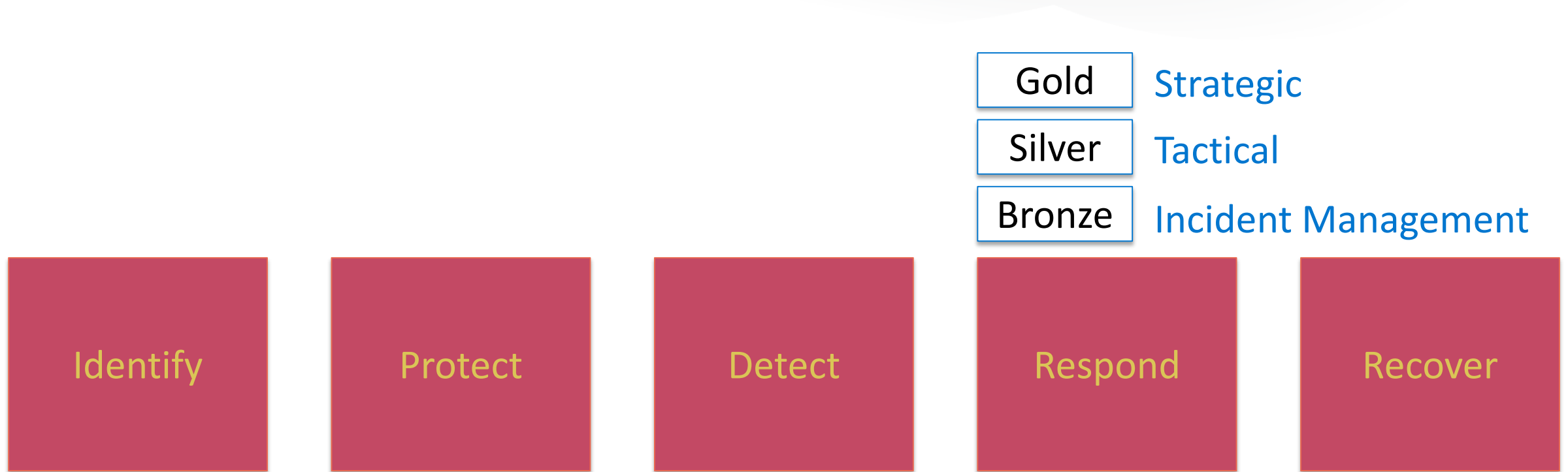
Have a go!

RSA[®]Conference2020

Why practice?

John

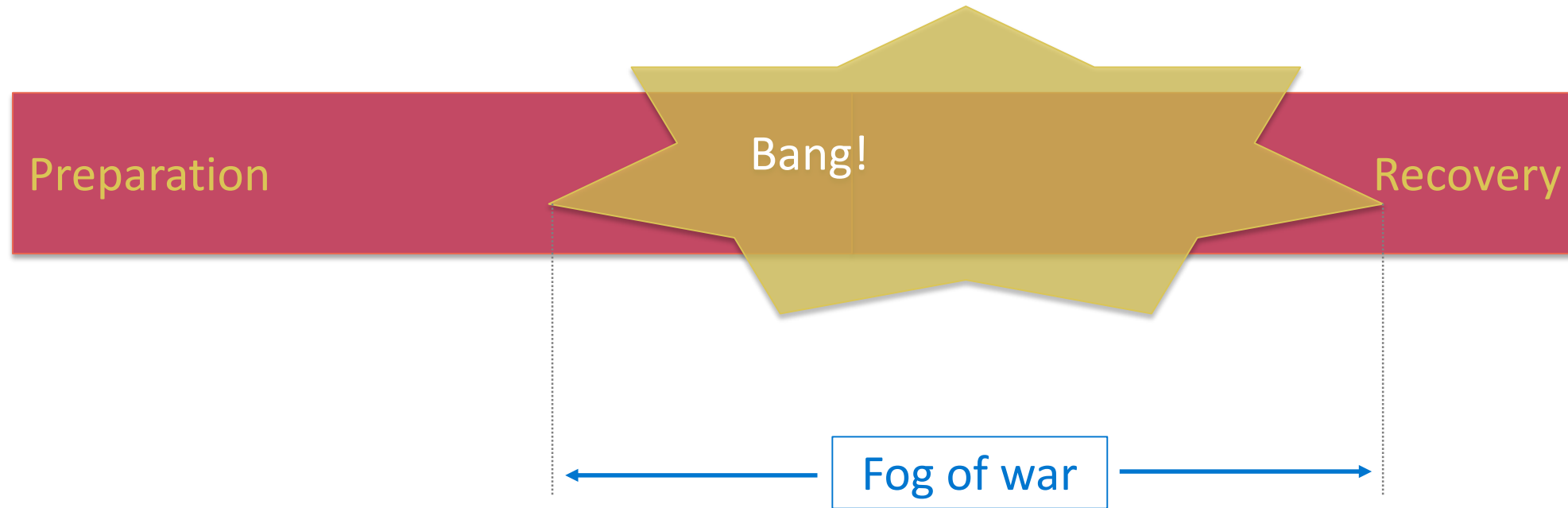
NIST cyber security framework



“Right of bang”



There really isn't just a bang



Why practice?

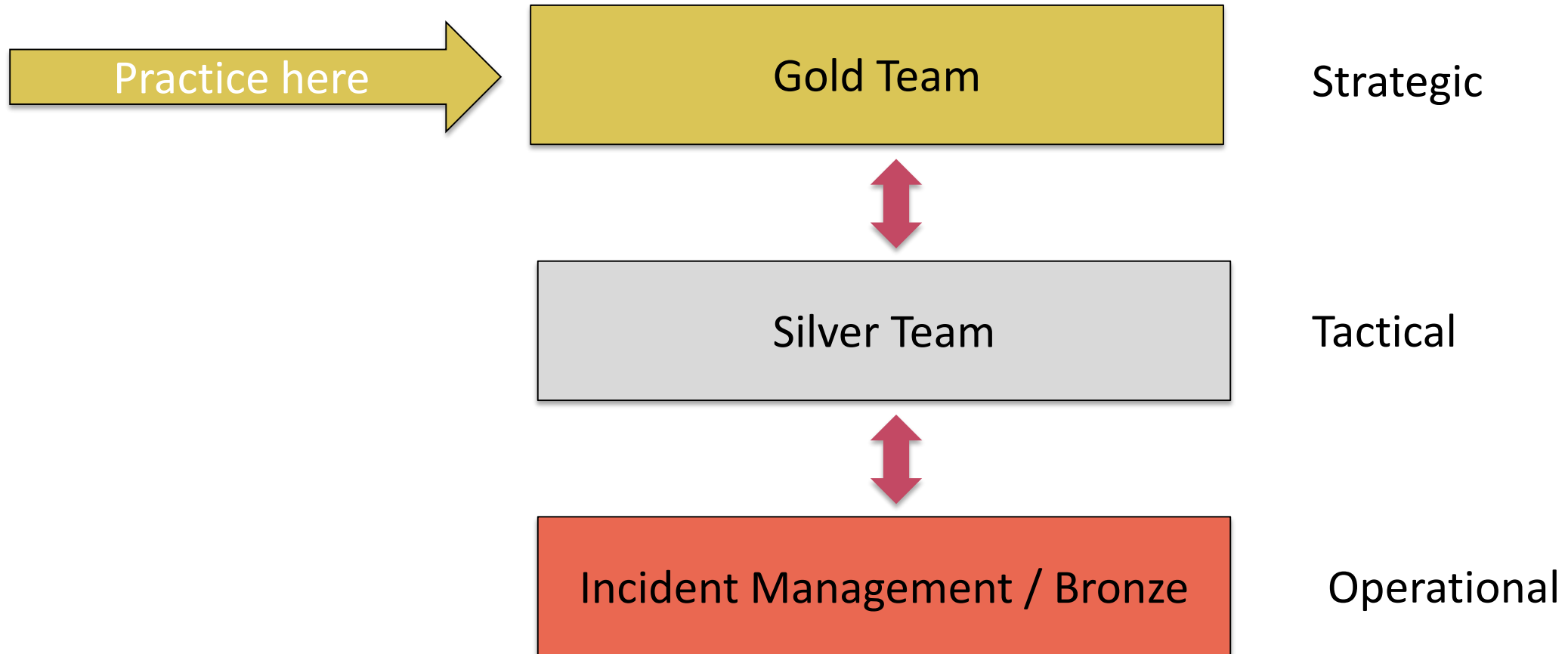
- Get the top team to actively think about this
 - It's not just a theoretical playbook or an IT issue
- It's better to make mistakes when the world isn't watching
- We all learn from mistakes 😊
- It's very trite but ...
- Personnel change frequently
- A control without assurance is not a control

RSA[®]Conference2020

Preparation

John

Typical incident management



Typical Gold Team members

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

Overcoming objections

We don't
have time

Incidents are
unknowable

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.

It won't
happen to us

We can do
this without
practice

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



RSA®Conference2020

Facilitation

Aaron

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 all 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

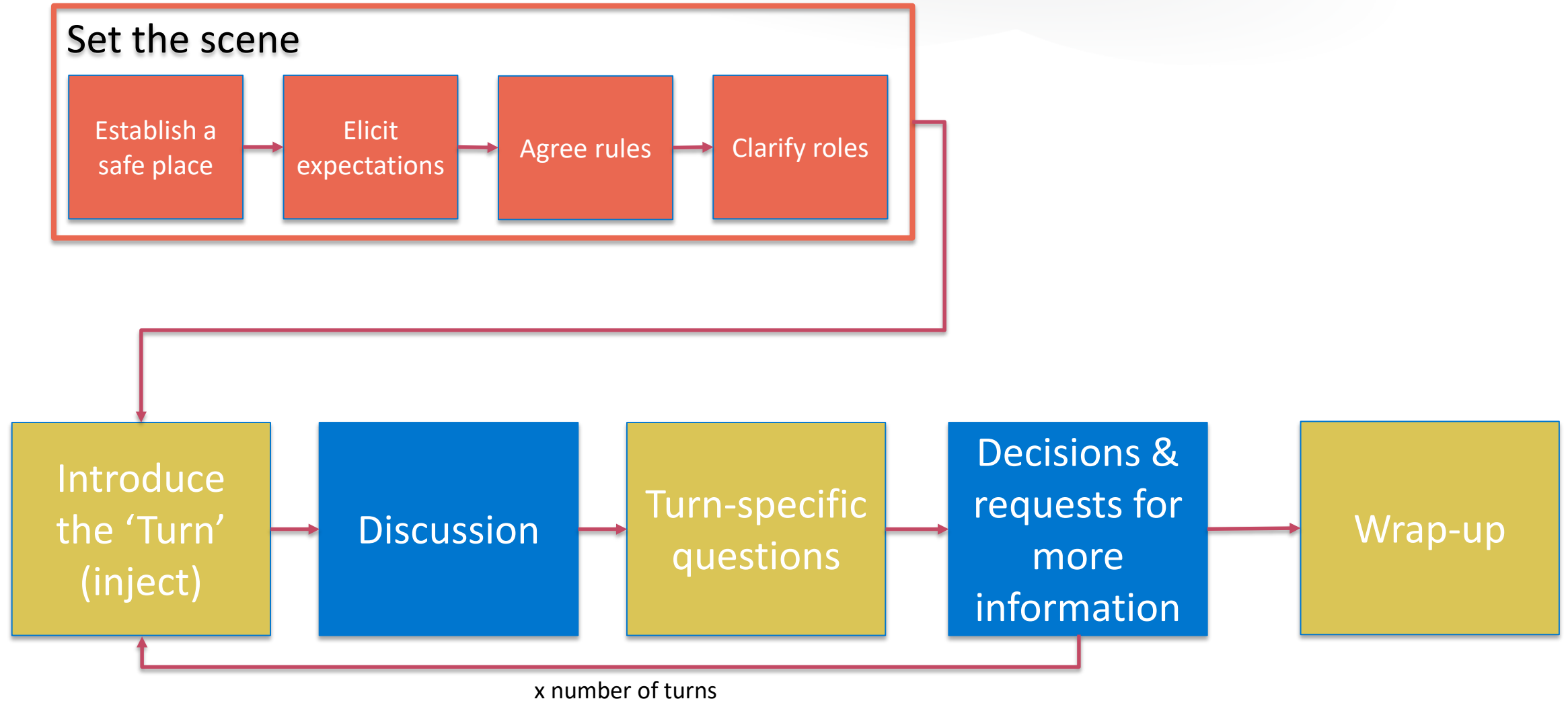
Car park



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

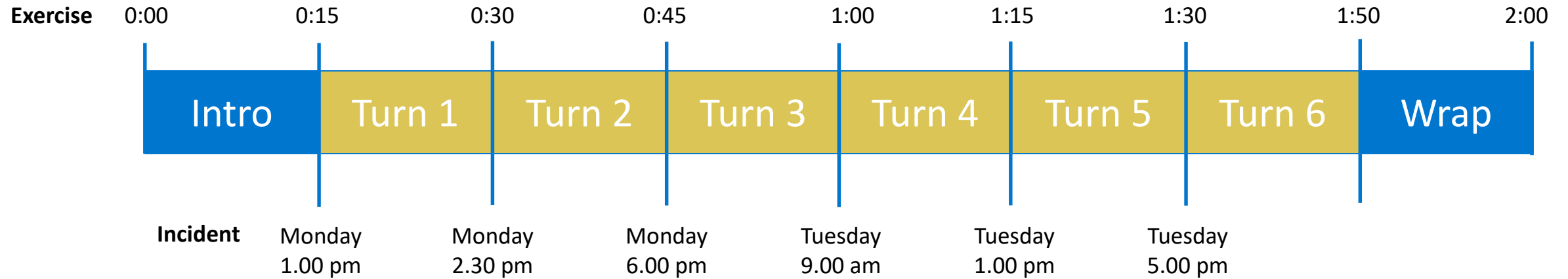
Structure of the exercise



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



RSA®Conference2020

What you need

John

Free to use, open-source resources

Introduction
slides

(Any scenario)

Facilitator
Overview and
Turns

(Scenario specific)

Turn slides

(Scenario specific)


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.

cybersecurityexercises.com – Free, Open Source



1: An email is received

MONDAY | 1:00 pm

- An email was sent to our Finance Director at 09:00 a.m. this morning. The sender claims to have direct access to our systems and to have extracted hundreds of thousands of our customer/3rd party details including credit card data.
- They say that unless they receive a ransom of \$500,000 paid in bitcoin ...
- Two deadlines:
 - Respond with intention by 3pm today
 - Pay the money by 1pm tomorrow
- If we don't pay, data will be released to the public

CYBERSECURITY EXERCISES

Open source resources for cybersecurity exercises

Home Facilitator Q&A Setting the Scene Exercises ▾ Contact Us About ↓

RSA[®]Conference2020

How to start an exercise

Aaron

Roles for the learning lab

- Facilitator
- Chief Executive Officer
- Chief Operating Officer
- Chief Financial Officer
- Head of IT or CISO
- 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 introduction (just for you)
2. Role launch
3. Turn handover

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 make people forget
- Share price

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 HR / CPO

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

Roles

Head of Legal / CLO

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

Head of Marketing / CMO

- 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 IT / CIO

- You care about:
 - IT infrastructure
 - IT Security →
 - User satisfaction
- Recovery of normal IT operations
- Do I get the blame for this?

or

Head of Information Security / CISO

- You care about:
 - Your team
 - Was this unexpected?
- Recovery of state
- Do we take the blame for this?

Roles

Scribe (groups of 9)

- You care about:
 - Documenting decisions
 - Legal cover
 - The next time
- You can help focus
 - “Can I just understand”

RSA®Conference2020

Let's do it!

You!

RSA[®]Conference2020

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.

RSA[®]Conference2020

Thank you

Aaron @ARosenmund | John @withoutfire

www.cybersecurityexercises.com

