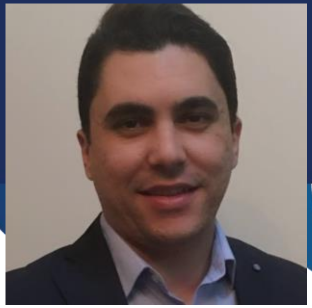
# Innovation & Tech Talk Online Event

# European Cybersecurity Month

## Navigating the Perfect Storm of a Cyber Crisis

19th October 2023



**Presenter**
**Ahmed Magdy**
**ISACA Young Professionals**

**Moderator**
**Matthias Kraft**
**Fidelity International**

**Co-Moderator**
**Somaye Hoseinpur**
**ISACA Young Professionals**

ISACA®
Germany Chapter

# Hinweise

- Dieses Event wird aufgezeichnet und zusammen mit etwaigen Handouts nach der Veranstaltung auf www.isaca.de zur Verfügung gestellt.
- Eine CPE-Bescheinigung wird ca. zwei Wochen nach dem Event an die von den Teilnehmern bei der Registrierung angegebene E-Mail-Adresse versendet.
- Fragen an den Presenter oder Moderator können über die Chat-Funktion gestellt werden.
- Feedback zum Event, Anregungen oder Wünsche bitte an: fg-innovation@isaca.de
- Der nächste TechTalk findet am 30. November 2023 zum Thema **Software Lifecycle meets Access Management** statt.
- Unsere Podcasts sind verfügbar unter: www.isaca.de/Podcasts

# Navigating the Perfect Storm of a Cyber Crisis

**Ahmed Magdy, Somaye Hoseinpur | FG Young Professionals**

October 2023

ISACA®
Germany Chapter

# FG Young Professionals

- ISACA Working Group for Young ISACA Members (< 38 years)
- Goal: Sharing expertise, discuss current subjects within the big ISACA topics
- What we are doing:
- Supporting the chapter‘s public relation activities
- Organising events
- This month‘s activity: European Cybersecurity Month

# Agenda

1. Setting the scene
2. Operational Resilience
3. What is a crisis?
4. Cyber Crisis Exercise Objectives
5. Cyber Crisis Exercise

# Setting the Scene

Russia-Ukraine War

Global geopolitical tension

38%

Avg weekly cyber attacks/organization increase in 2022 vs 2021*

$4.35 Million

The average total cost of data breaches in 2022 was $4.35 million, according to the IBM/Ponemon Institute report

* Check Point Research Reports

# What is Operational Resilience?

1 X 3

Crisis Management – preventing or minimizing the impact of crises

Business Continuity - protecting the customer experiences that matter

Emergency Response – protecting all our assets at all our Sites

# What is a Crisis?

An abnormal and unstable situation that threatens the organization’s strategic objectives, reputation or viability and which requires a response which is beyond the normal business as usual structure and / or resources

**Priorities:**

Saving lives and ensure people safety

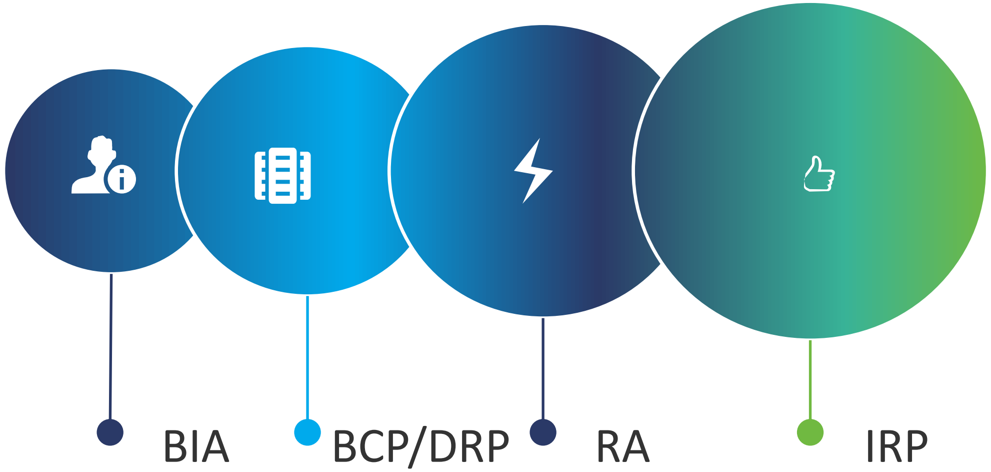
Minimize the damage

Return to normal operations

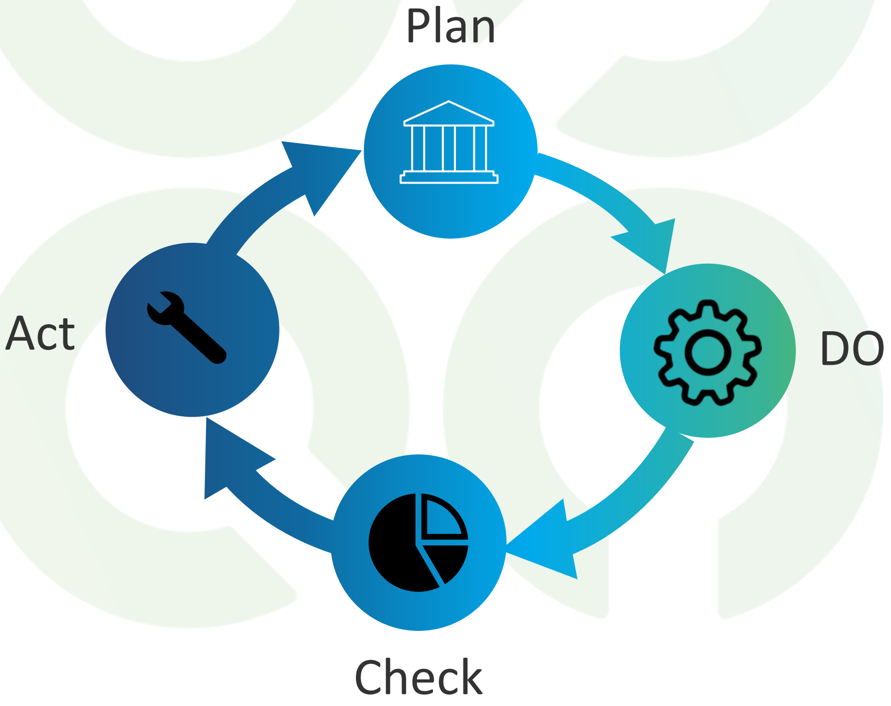
Protect the organization’s reputation

# Getting Ready

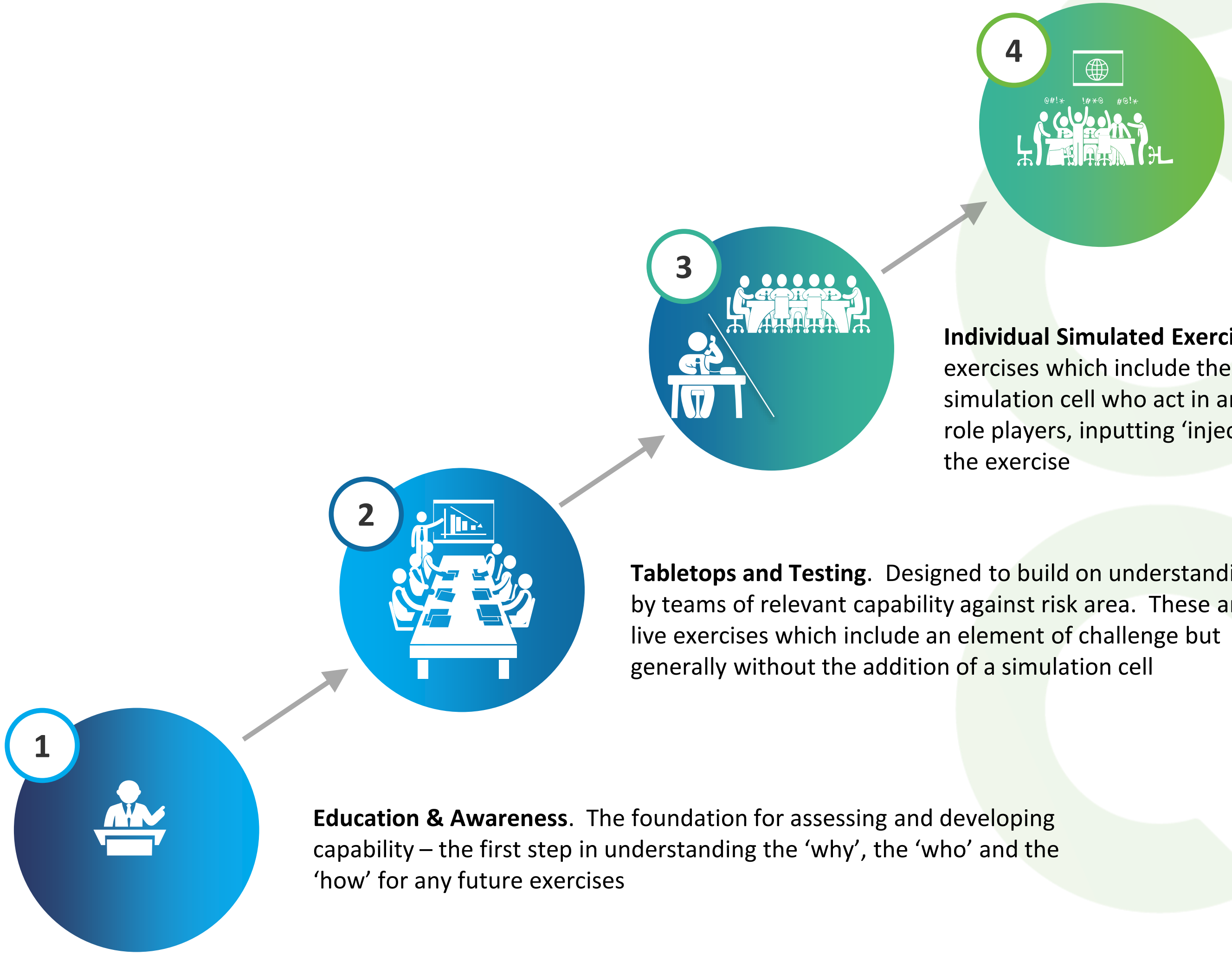
## Key Inputs



## Approach



# Cyber Crisis Readiness



**Education & Awareness**. The foundation for assessing and developing capability – the first step in understanding the ‘why’, the ‘who’ and the ‘how’ for any future exercises

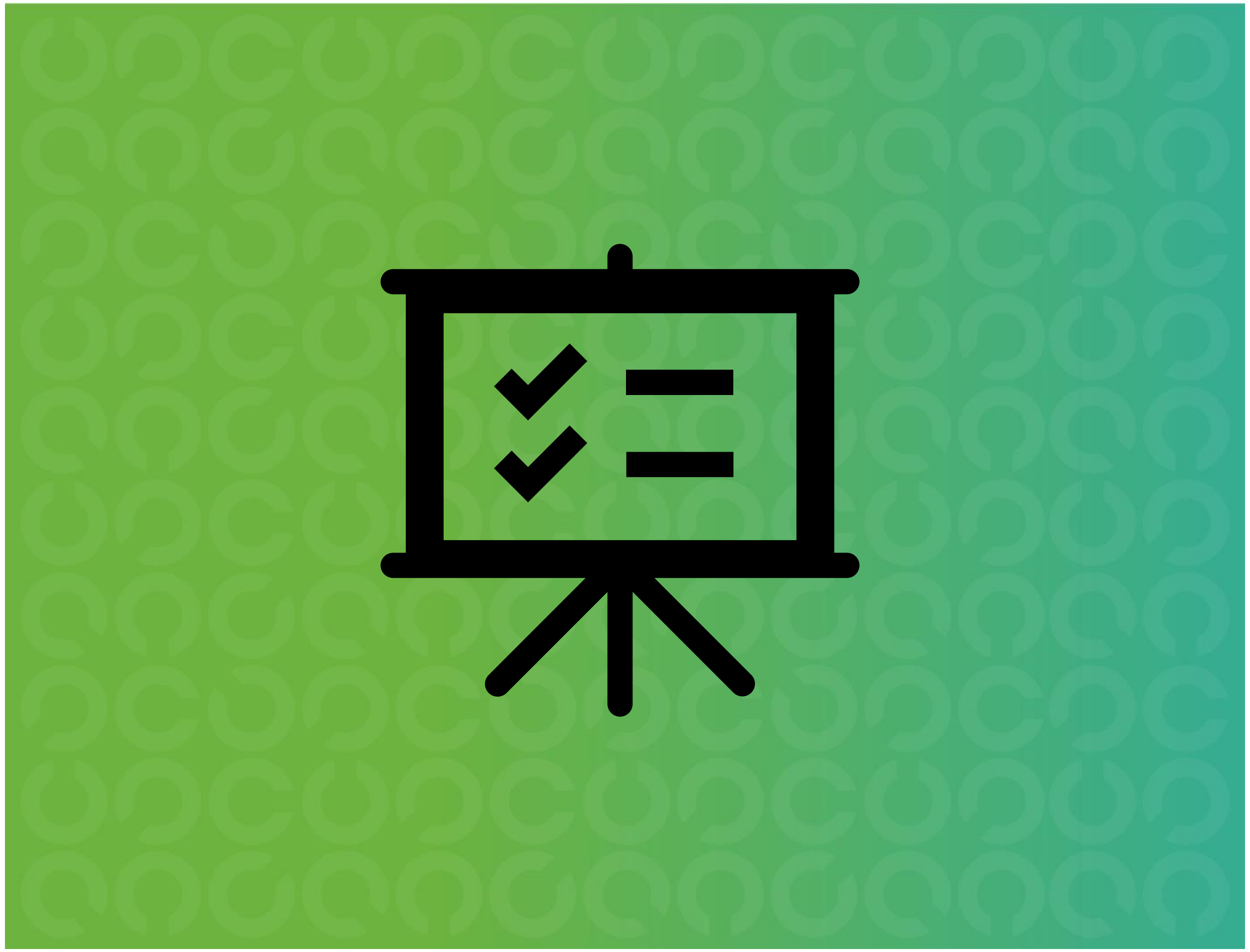
**Tabletops and Testing**. Designed to build on understanding by teams of relevant capability against risk area. These are live exercises which include an element of challenge but generally without the addition of a simulation cell

**Individual Simulated Exercise (SIMEX)**. Live exercises which include the addition of a simulation cell who act in an adversarial capacity as role players, inputting ‘injects’ of information into the exercise

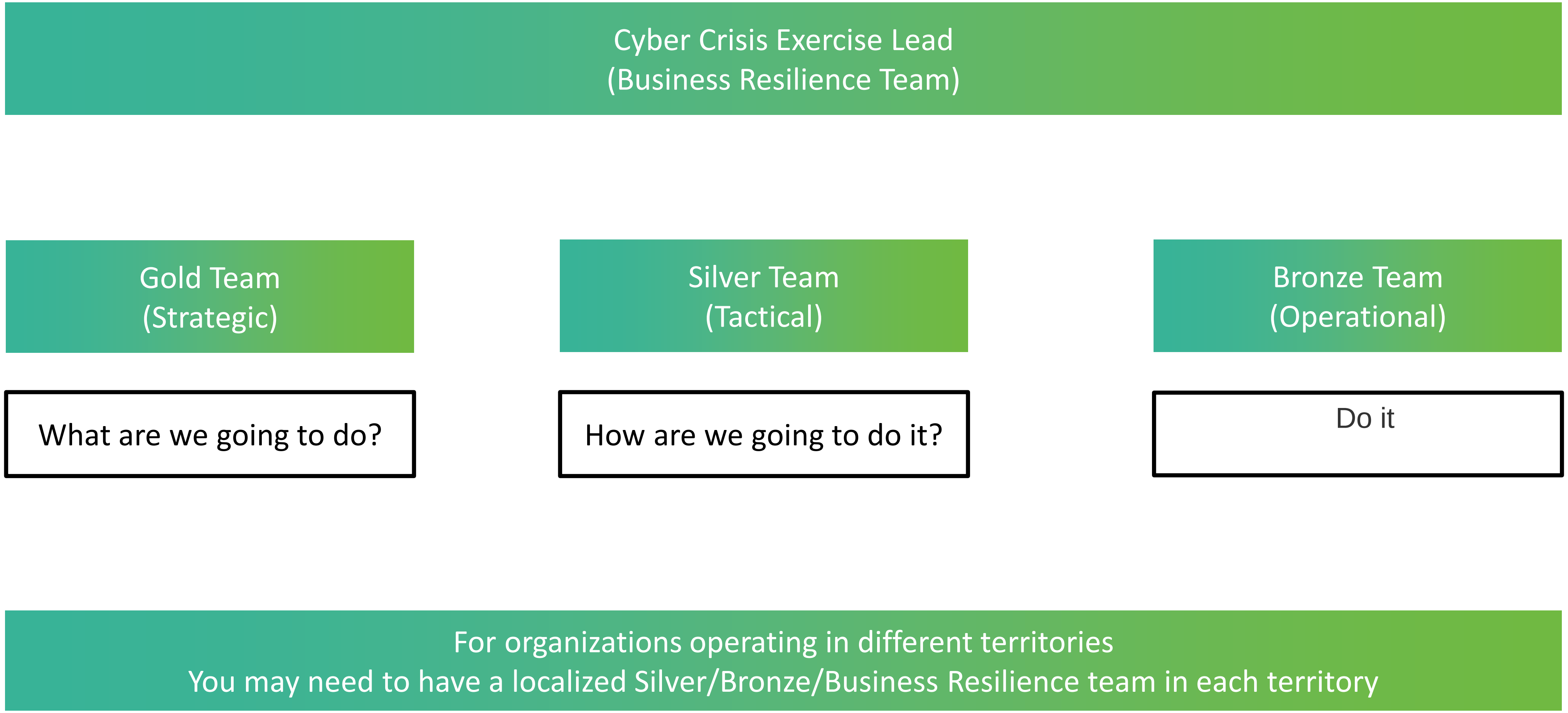
**Complex SIMEX**. All of the live simulation and role-playing but including multiple exercise teams linking up as they exercise their response

# Cyber Crisis Exercise Objectives

- Simulate a **significant impact to corporate systems, customer facing products** and platforms and ultimately reputation
- **Rehearse roles and responsibilities** during an attack and decision making.
- Understand **what we would or wouldn’t be prepared to switch-off** to contain an attack
- Understand  ransomware attacks negotiation.
- Rehearse **crisis communications** for a cyber attack
- Understand the organization **Business Continuity capability**



# Cyber Crisis Team



Cyber Crisis Exercise Lead
(Business Resilience Team)

Gold Team
(Strategic)

What are we going to do?

Silver Team
(Tactical)

How are we going to do it?

Bronze Team
(Operational)

Do it

For organizations operating in different territories
You may need to have a localized Silver/Bronze/Business Resilience team in each territory

**Crisis Management Team**

- Initiate the exercise
- High level coordination
- Record observations for improvements

**Gold Team**

- Overall strategic command
- Make critical decisions and set business priorities and direction.

**Silver Team**

- Liaise between Gold and Bronze teams.
- Escalate to Gold team
- Respond to Gold team inquiries.
- Communicate decisions and directions to the Bronze team

**Bronze Team**

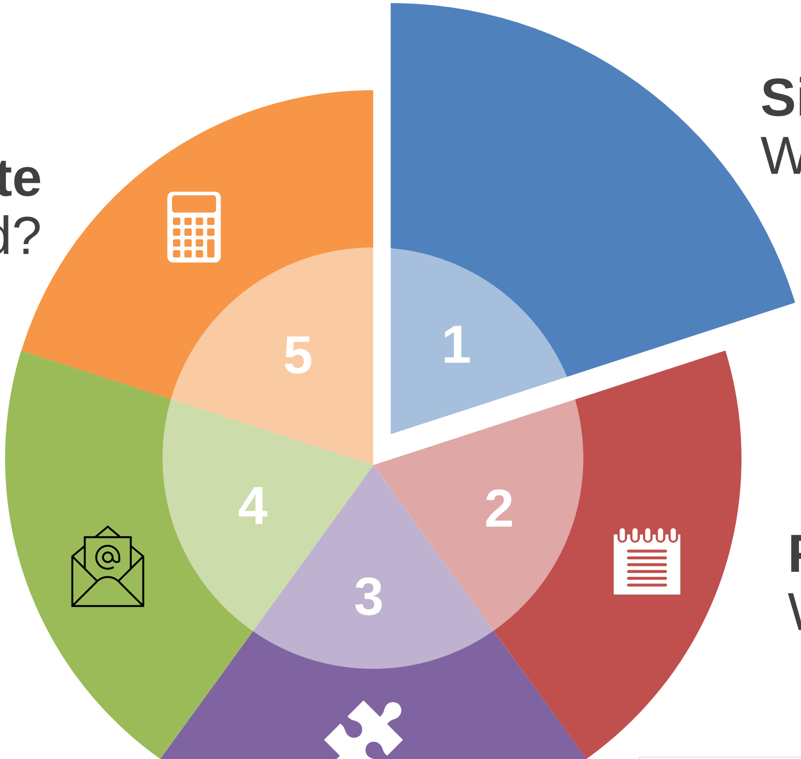
- Send Regular comms in a timely manner.
- Provide answers to questions raised by Gold and Silver
- Fixing the problem.

# Cyber Crisis Action Time

**CISA Cyber Crisis Scenarios**

# Live Response

<u>SPACE</u> (**S**ituation, **P**riorities, **A**ctions, **C**omms, **E**valuate)



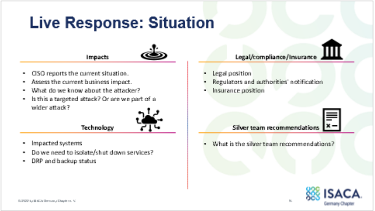
**Situation**
What is going on?

**Priorities**
What are the objectives?

**Actions**
What should we do?

**Comms**
Who should be informed?

**Evaluate**
Where do we stand?



## Live Response: Situation

**Impacts**

- CISO reports the current situation.
- Assess the current business impact.
- What do we know about the attacker?
- Is this a targeted attack? Or are we part of a wider attack?

**Technology**

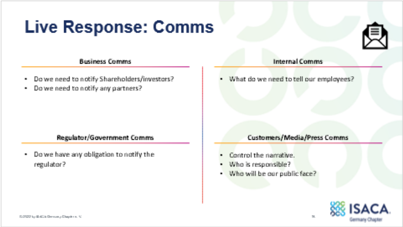
- Impacted systems
- Do we need to isolate/shut down services?
- DRP and backup status

**Legal/compliance/Insurance**

- Legal position
- Regulators and authorities' notification
- Insurance position

**Silver team recommendations**

- What is the silver team recommendations?



## Live Response: Comms

**Business Comms**

- Do we need to notify Shareholders/investors?
- Do we need to notify any partners?

**Regulator/Government Comms**

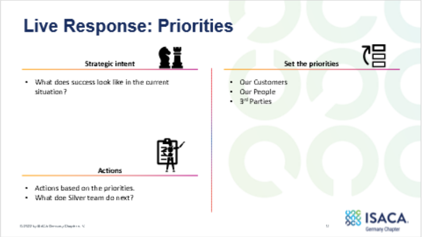
- Do we have any obligation to notify the regulator?

**Internal Comms**

- What do we need to tell our employees?

**Customers/Media/Press Comms**

- Control the narrative.
- Who is responsible?
- Who will be our public face?



## Live Response: Priorities

**Strategic intent**

- What does success look like in the current situation?

**Actions**

- Actions based on the priorities.
- What doe Silver team do next?

**Set the priorities**

- Our Customers
- Our People
- 3rd Parties

# Live Response: Situation

## Impacts

- CISO reports the current situation.
- Assess the current business impact.
- What do we know about the attacker?
- Is this a targeted attack? Or are we part of a wider attack?

## Technology

- Impacted systems
- Do we need to isolate/shut down services?
- DRP and backup status

## Legal/compliance/Insurance

- Legal position
- Regulators and authorities' notification
- Insurance position

## Silver team recommendations

- What is the silver team recommendations?

# Live Response: Priorities

## Strategic intent

- What does success look like in the current situation?

## Set the priorities

- Our Customers
- Our People
- 3rd Parties

## Actions

- Actions based on the priorities.
- What doe Silver team do next?

# Live Response: Comms

### Business Comms

- Do we need to notify Shareholders/investors?
- Do we need to notify any partners?

### Internal Comms

- What do we need to tell our employees?

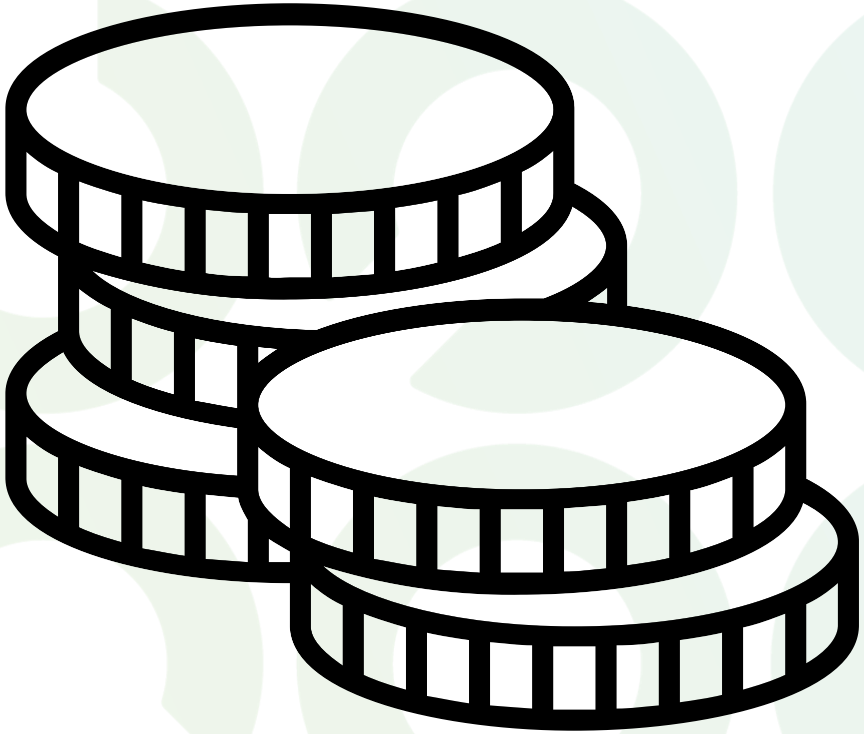
### Regulator/Government Comms

- Do we have any obligation to notify the regulator?

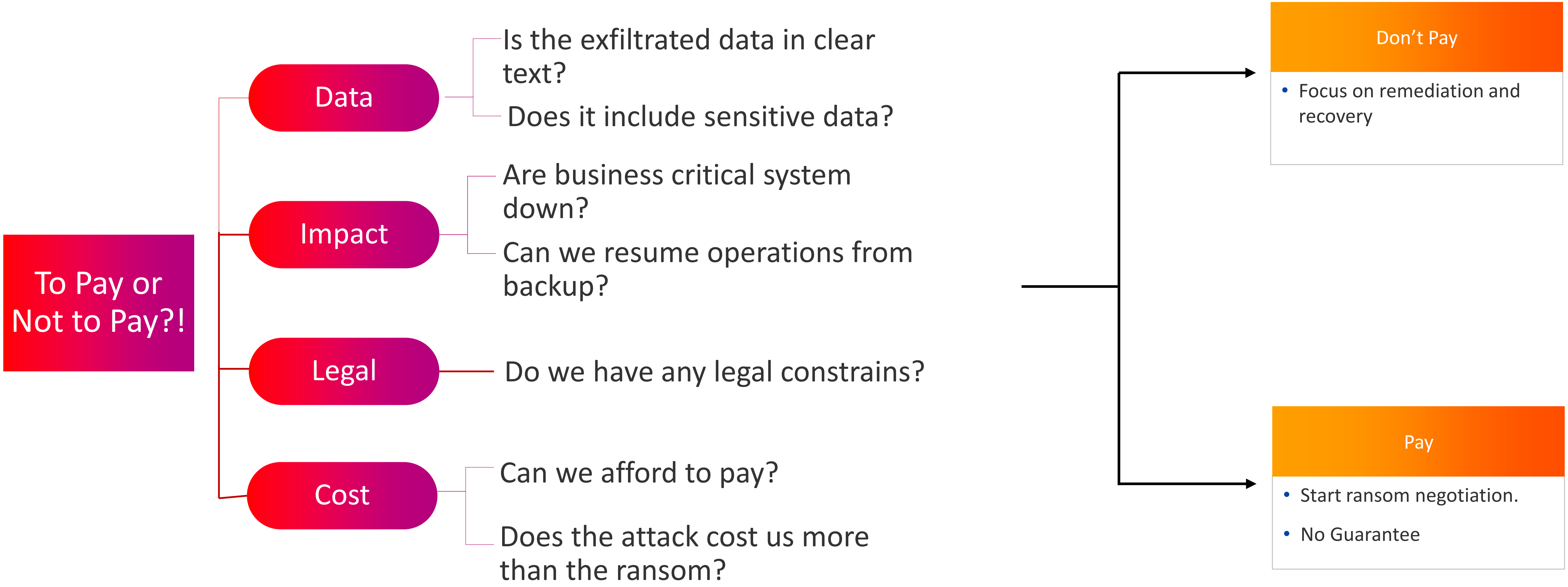
### Customers/Media/Press Comms

- Control the narrative.
- Who is responsible?
- Who will be our public face?

# Should we pay the ran$om?



# Should we pay the ran$om?



To Pay or Not to Pay?!

Data
- Is the exfiltrated data in clear text?
- Does it include sensitive data?

Impact
- Are business critical system down?
- Can we resume operations from backup?

Legal
- Do we have any legal constrains?

Cost
- Can we afford to pay?
- Does the attack cost us more than the ransom?

Don’t Pay
- Focus on remediation and recovery

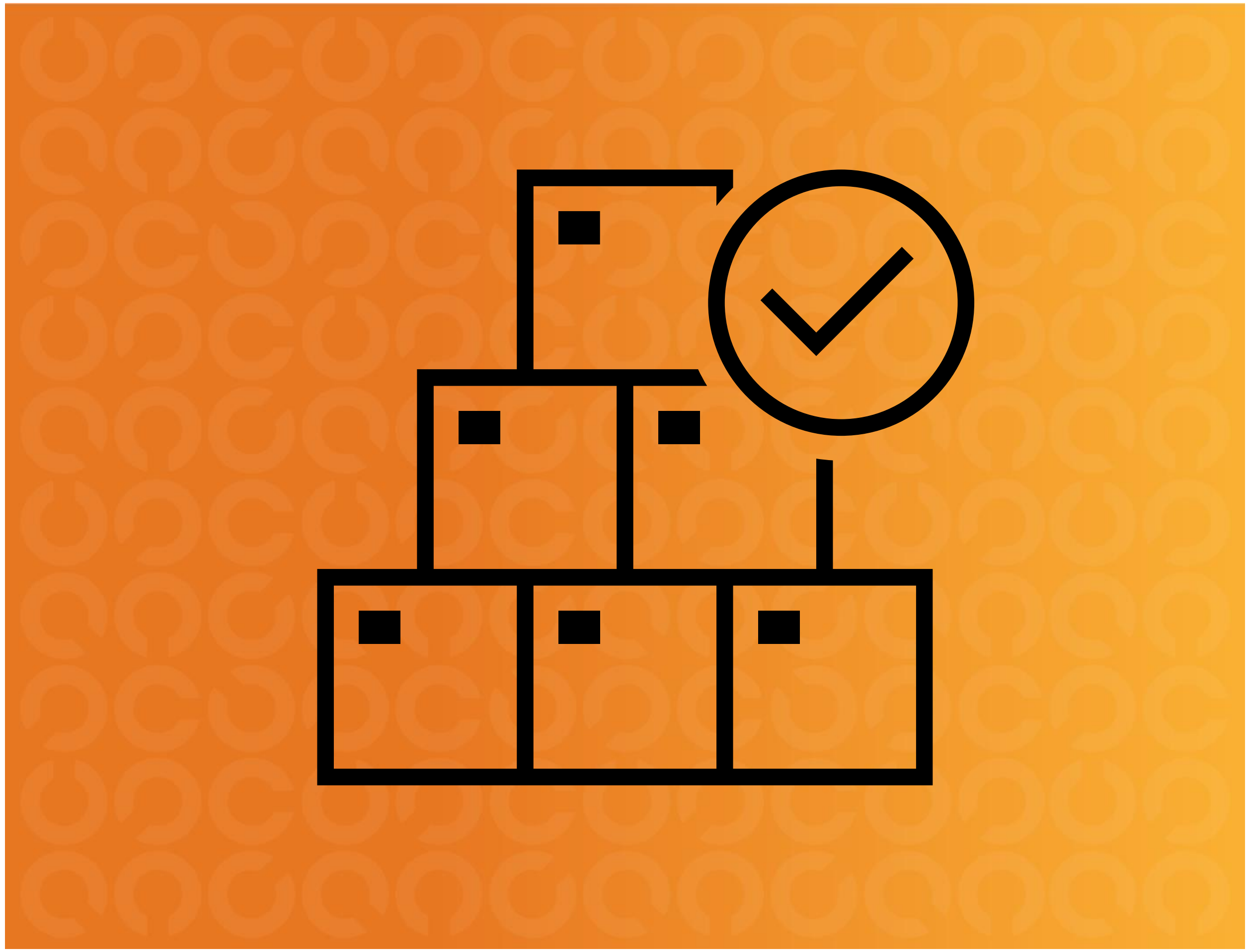
Pay
- Start ransom negotiation.
- No Guarantee

# Cyber Crisis Exercise Pitfalls

- Crisis Leads optimism bias
- The size of the team can be a challenge
- Inconsistent team meeting's structure
- Insufficient comms between Gold/Silver/Bronze teams.
- Failure to explicitly define what success looks like?
- Lack of clarity on decision making.
- Silver shifts focus from business side to technical issues.
- Lack of collaboration between teams
- Ignoring the media/press.

# What is a good exercise looks like?

- Good collaboration between teams.
- Decisions are made in a timely manner.
- Effective and timely manner comms.
- clear and consistent inputs to Silver and Gold regarding worst-case impacts.
- clearly explaining the risks and impacts to the business.
- Restoring the business operations in a timely manner.
- Lessons learned and improvements are captured.



# Q & A

# THANK YOU

ISACA®

Germany Chapter