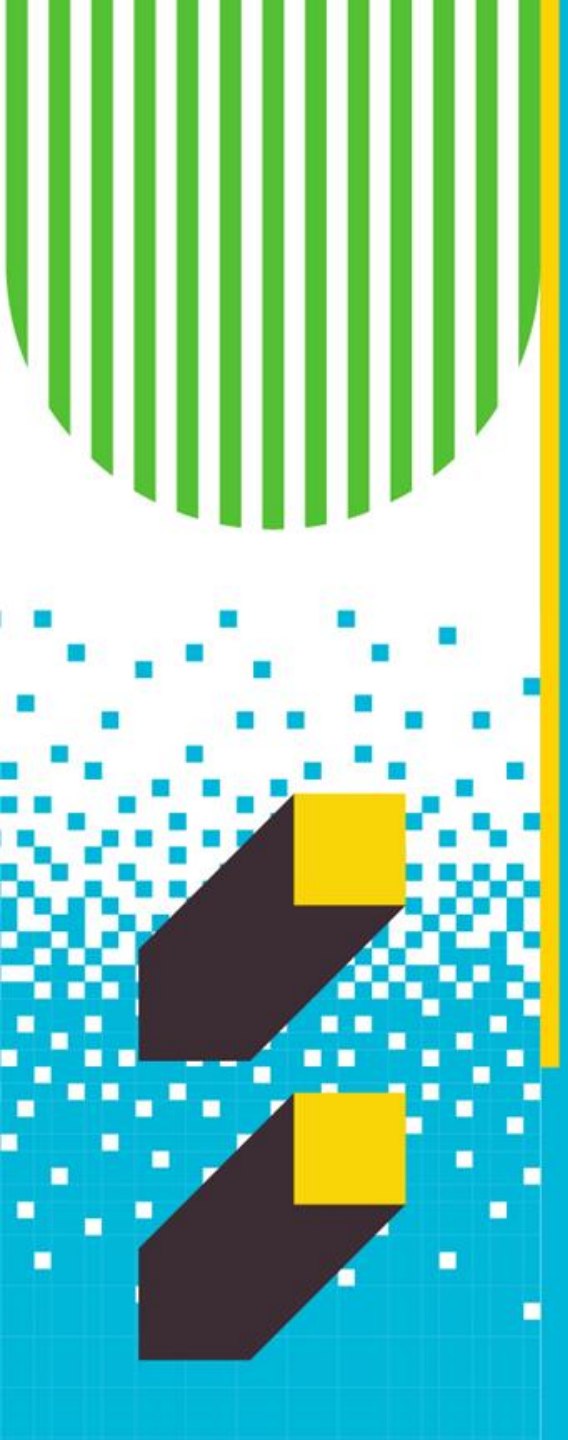


IAPP **Privacy. Security. Risk. 2025**

Training 28-29 October

Workshops 29 October

Conference 30-31 October

SAN DIEGO

#PSR25

The Breach War Room

Interactive Crisis Stimulation

Real-world breach scenario

decision-making under pressure

#PSR25

WELCOME AND INTRODUCTIONS

Mandy Lit
Director, Privacy and Compliance
Global Enterprises &
High-Growth Tech

Ali Abbas-Hirji
VP and Cybersecurity Professor at
Computek College

Noemi Chanda
Partner, Digital Trust & Privacy
Deloitte

AGENDA OUTLINE

1. **Welcome & Introductions**
   Team formation and context setting
2. **Scenario Overview**
   LegalBeagle breach situation briefing
3. **Simulation Stages (1–4)**
   Progressive decision points under pressure
4. **Reflection Pauses (Stage 5)**
   Cross-team comparison and analysis
5. **Tools & Frameworks**
   Practical resources for implementation
6. **Key Takeaways**
   Actionable insights and lessons learned

Q&A

Pre-TTX: Goals of Tabletop Exercise

Enhanced Awareness

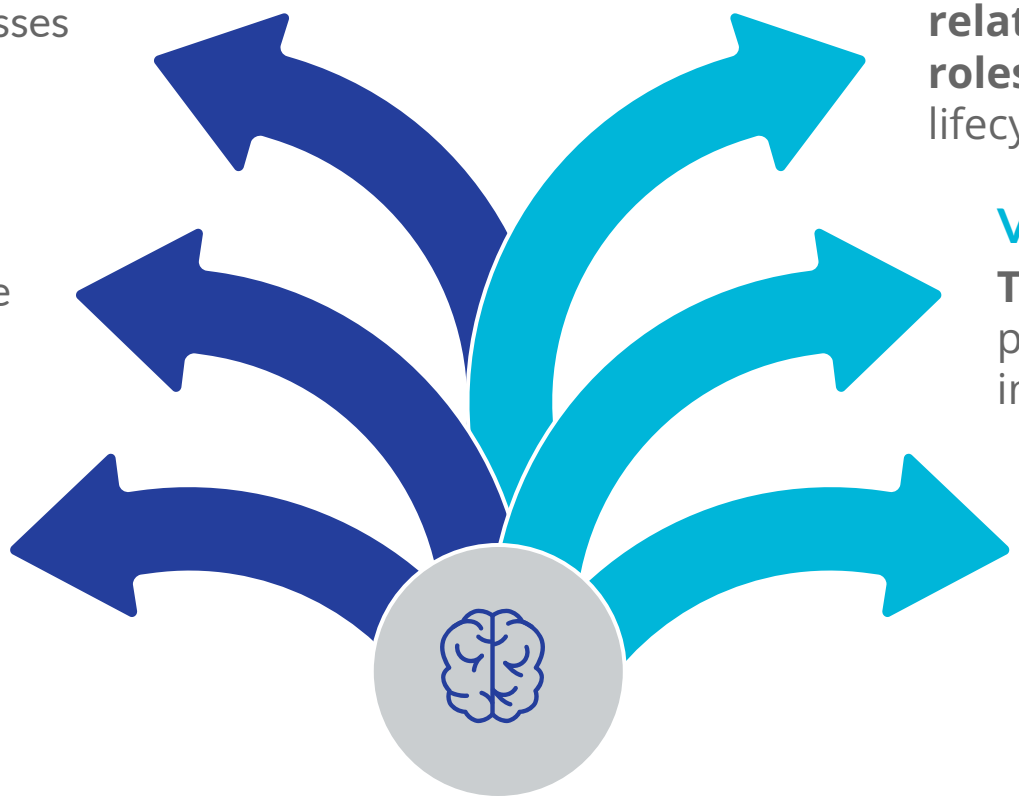
Improve understanding of existing cyber incident response processes and procedures

Service Continuity

Evaluate and enhance capacity to ensure uninterrupted service in the event of an incident

Role Coordination

Understand individual roles in coordinating response with evolving incomplete information



Key Insights

Gain deeper insight into **cyber-related issues and stakeholder roles** across the incident response lifecycle

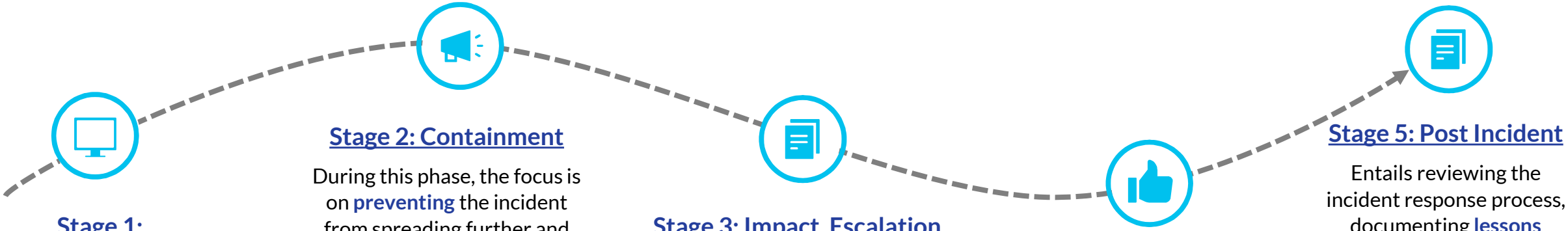
Validated Communication

Test and verify communication plans during a data breach incident

Threat Exploration

Explore specific **threats, risks, challenges, and key considerations** in cyber incident response

Pre-TTX: Key stages of this TTX



Stage 1: Identification

The initial phase involves the discovery of potential security incidents, including the **detection of anomalous activities,** threats, or vulnerabilities within the organization's network or systems.

Stage 2: Containment

During this phase, the focus is on **preventing** the incident from spreading further and limiting its impact. Immediate actions are taken to **isolate affected systems** or components to prevent further damage or unauthorized access.

Stage 3: Impact, Escalation, and External Reporting

Entails further analysis of the extent and nature of the impact, as well as internal and external **reporting obligations**, including regulatory and contractual notifications, media communications, and reporting to **key stakeholders and the board**

Stage 4: Recovery

In this stage, the objectives are to: i) completely **remove the root cause** of the incident from the affected systems or environment and ii) **restore affected systems,** services, and operations to their usual state, ensuring that business functions return to normalcy while verifying system integrity.

Stage 5: Post Incident

Entails reviewing the incident response process, documenting **lessons learned,** and implementing enhancements to bolster overall security and resilience.

Note that the stages above may unfold concurrently – the implications of an incident may be felt immediately, but containment and recovery may span months or even years.

Pre-TTX: Key definitions & TTX roles

Event - An event is an exception to the normal operation of IT infrastructure, systems, or services. Not all events become incidents.

Incident - A security incident is defined as an adverse event that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system. Not all incidents become privacy breaches.

Participants

- **Actively engage** in scenario discussions and make decisions as they would in a real incident. Collaborate with other participants to coordinate actions and solve problems presented in the exercise.

Observers

- **Monitor the exercise** without directly participating in discussions or decision-making, taking notes on actions, decisions, and communication for later analysis.

Advisors

- **Offer expert guidance**, technical input, or clarification on specific issues when requested, supporting participants.

Scenario Background

A critical incident simulation for a cloud-based case management platform.

The Organization

Legalbeagle LLC
Cloud Based Case Management Platform

Mid-sized legal technology company **500+** firms

Handles sensitive client data daily

The Challenge

Suspicious Activity Detected
Anomalies detected across multiple systems with unclear scope and impact

Cross Functional Response
Navigate crisis with incomplete information under extreme time pressure

72hr Window

Balance thoroughness with speed while managing **stakeholder expectations** and **regulatory requirements**

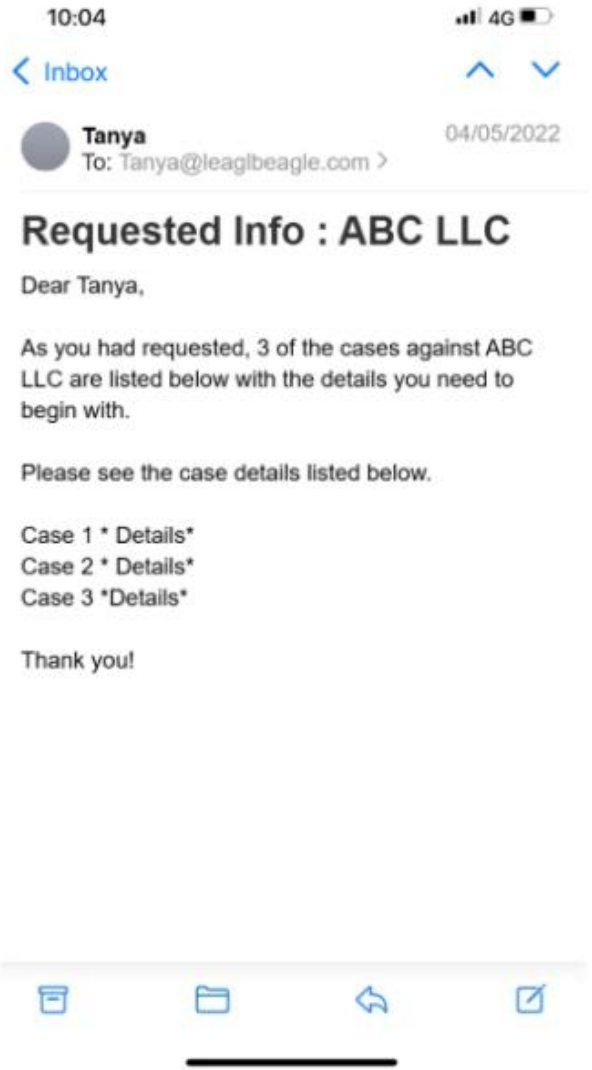
Stage 1: Detection & Response

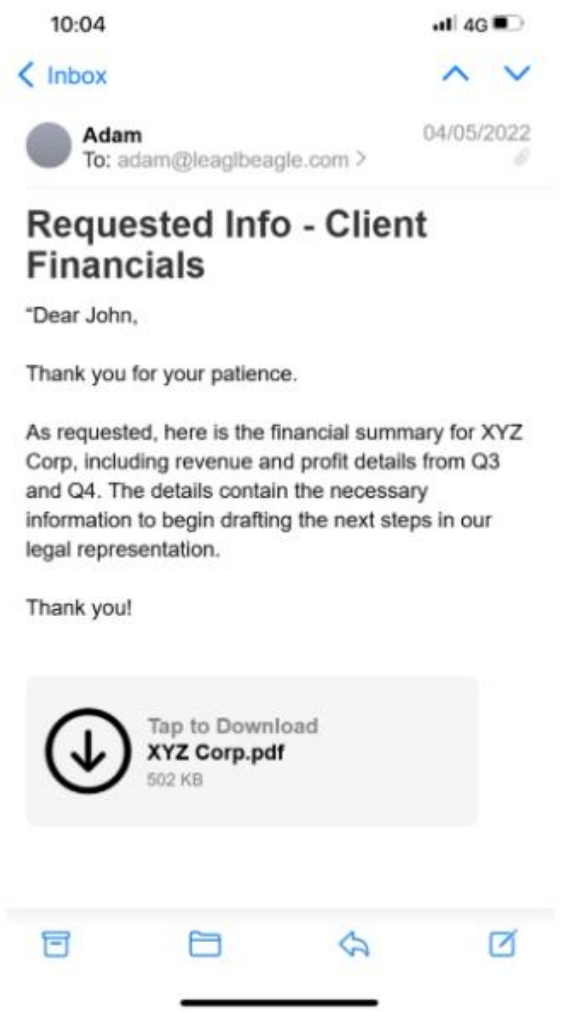
Employee report- unusual system behavior and unexpected access patterns

Network analysis- suspicious outbound traffic to unknown external servers

Escalate immediately with limited information or **wait for evidence** with time pressure?

Prompt 1





An email has been received with unexpected sensitive information included by the GenAI assistant. IT is called to investigate the incident. What is your first step?

Prompt 2

Timestamp: 03/29/2022 14:22:31 UTC
Request ID: 43567421
User: john@leaglebeagle.com
Request Type: GET
Endpoint: /case-update?case=XYZ-Corp
Request Parameters: case=XYZ-Corp
Action Taken: Retrieved case details for XYZ-Corp
Response Code: 200 (Success)
Suspicious Action: Unauthorized automated email trigger after retrieval of case details.

Application Server Log 2:

Timestamp: 03/30/2022 10:10:14 UTC
Request ID: 43567422
User: internal-system@leaglebeagle.com
Request Type: POST
Endpoint: /send-case-report
Request Parameters: case=XYZ-Corp, recipient=tanya@leaglebeagle.com, data=Q1-Q4-Report
Action Taken: Sent case report email to tanya@leaglebeagle.com
Response Code: 200 (Success)
Suspicious Action: Internal system triggered email send without explicit user authorization.

What logs and data sources will you review to understand why sensitive data was leaked?

Stage 2: Containment Decisions

Data Exposure Risk

Customer data potentially compromised- scope and severity unknown

Regulatory Clock

72-hr notification window regulator inquiry imminent

Containment Dilemma

System shutdown vs forensic preservation

How do you balance business continuity with evidence preservation?

Prompt 3

Other departments are now receiving similar sensitive data leaks in their emails. What actions will you take to prevent further spread?

Stage 3: Escalation & External Pressure

Decision Crossroads

Notify stakeholders with partial facts or **wait for complete confirmation** while pressure mounts

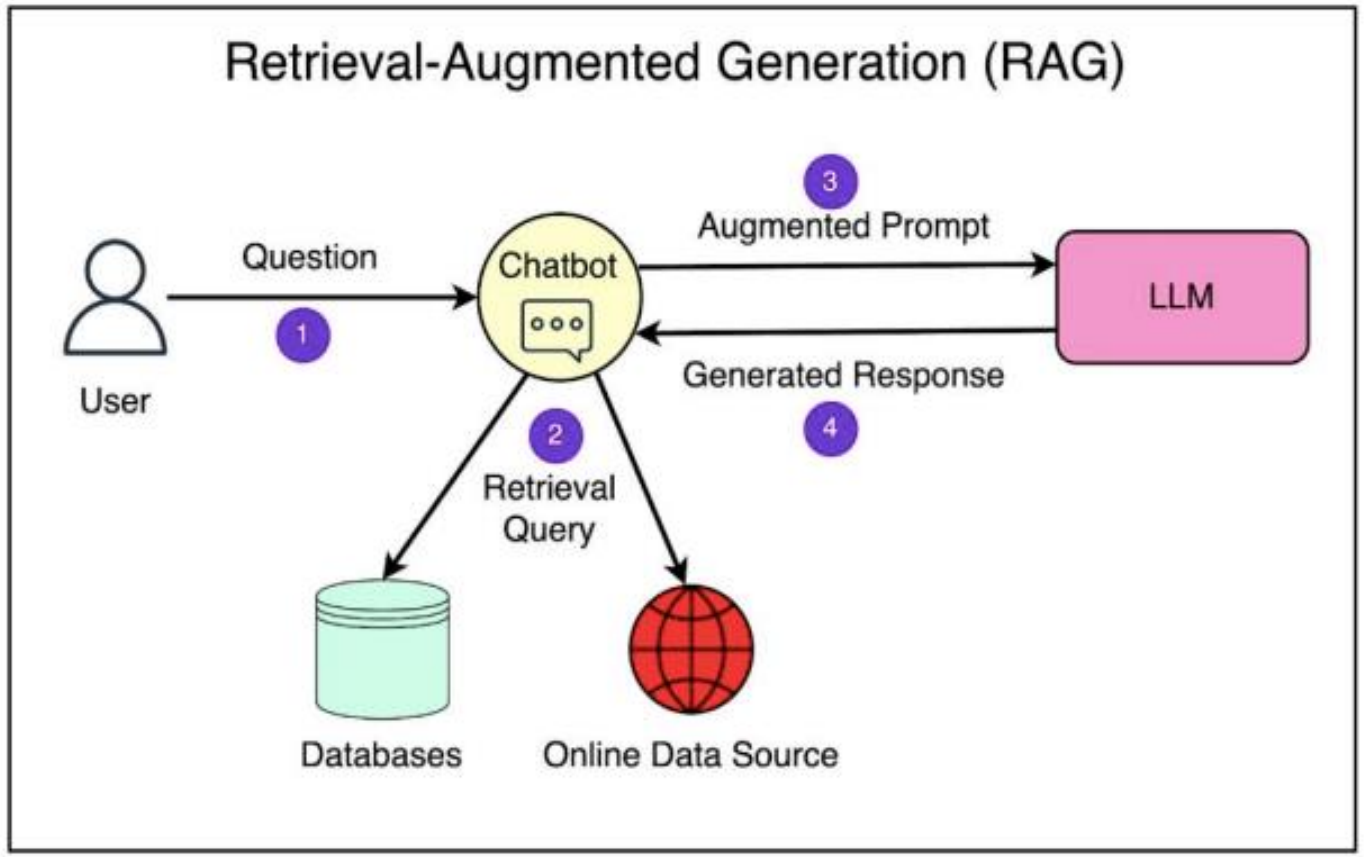
Media Attention

Journalist inquiry about rumored data leak - **reputation at stake**

Client Demands

SLA obligations require **immediate notification** of security events

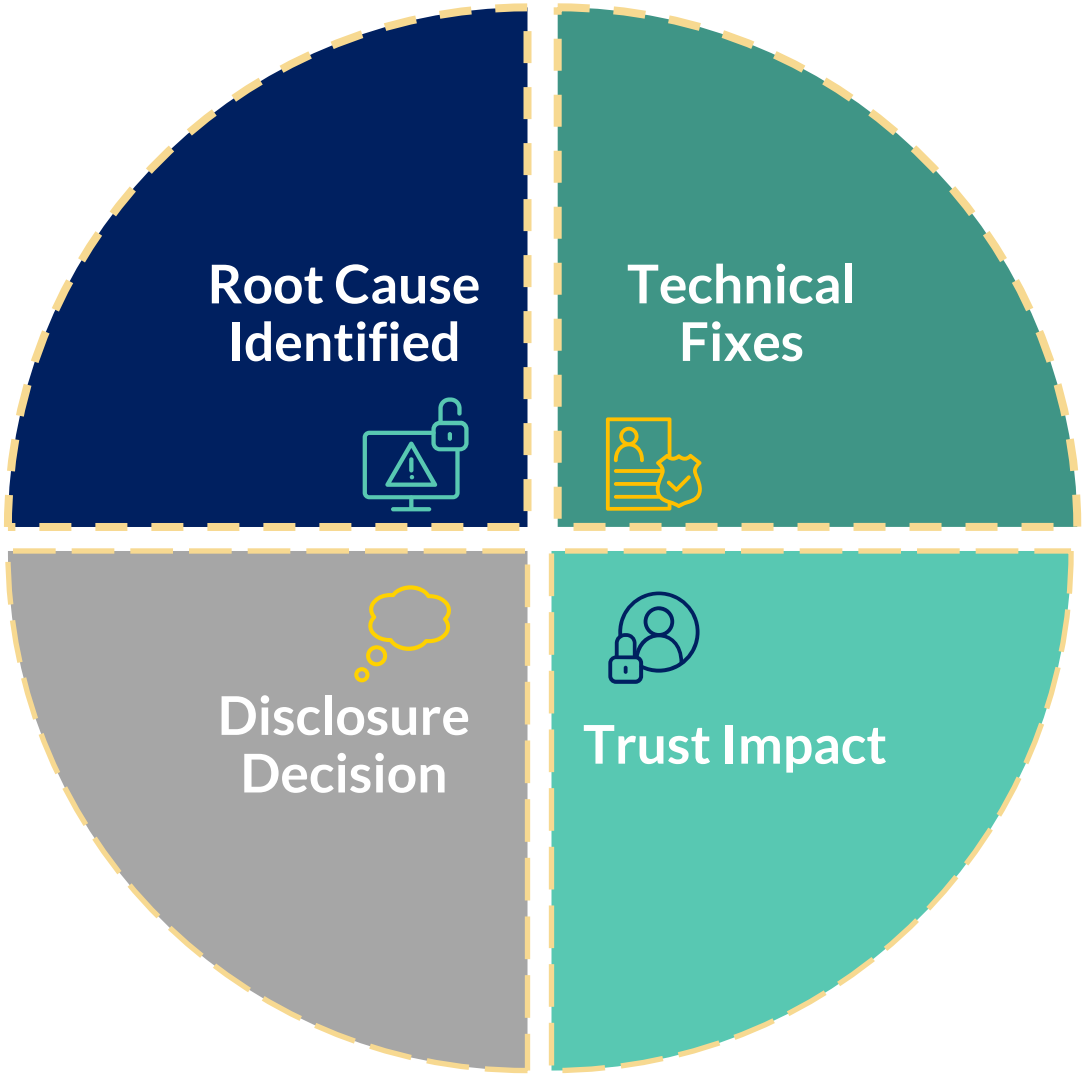
Prompt 4



You identify that the root cause involves a prompt injection due to an adversarial prompt embedded in the RAG. What measures will you implement to remove the prompt and prevent future occurrences?

Stage 4: Root Cause & Recovery

Cloud misconfiguration exposed customer data repositories



Remediation underway - systems being secured and monitored

Public disclosure now or after remediation?

Client confidence shaken - relationship management critical

Stage 5: Post-Incident Reflection Points…

Escalation Threshold Differences

Security vs Privacy vs Legal - where did teams diverge on when to act?

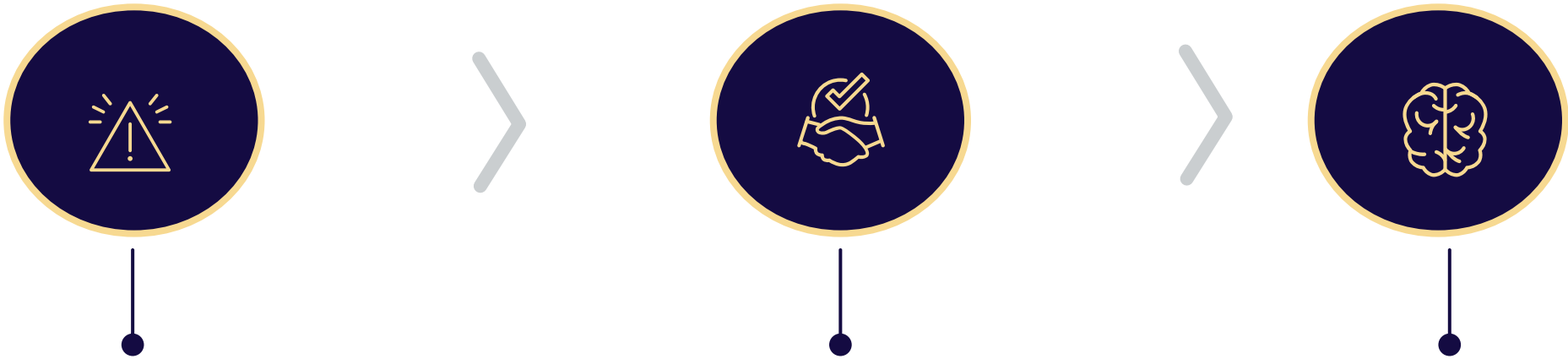
Conflicting Organization Goals

Containment vs Notification vs Liability - how do competing priorities play out?

Media Pressure Response

Reputation vs Compliance vs Risk - how did functions prioritize under external scrutiny?

RESOURCE LIST



Breach Classification Matrix

Standardized framework for categorizing incident severity and required response protocols

• NIST Incident Response Framework
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

RACI Coordination Template

Clear responsibility assignments for Responsible, Accountable, Consulted, and Informed roles

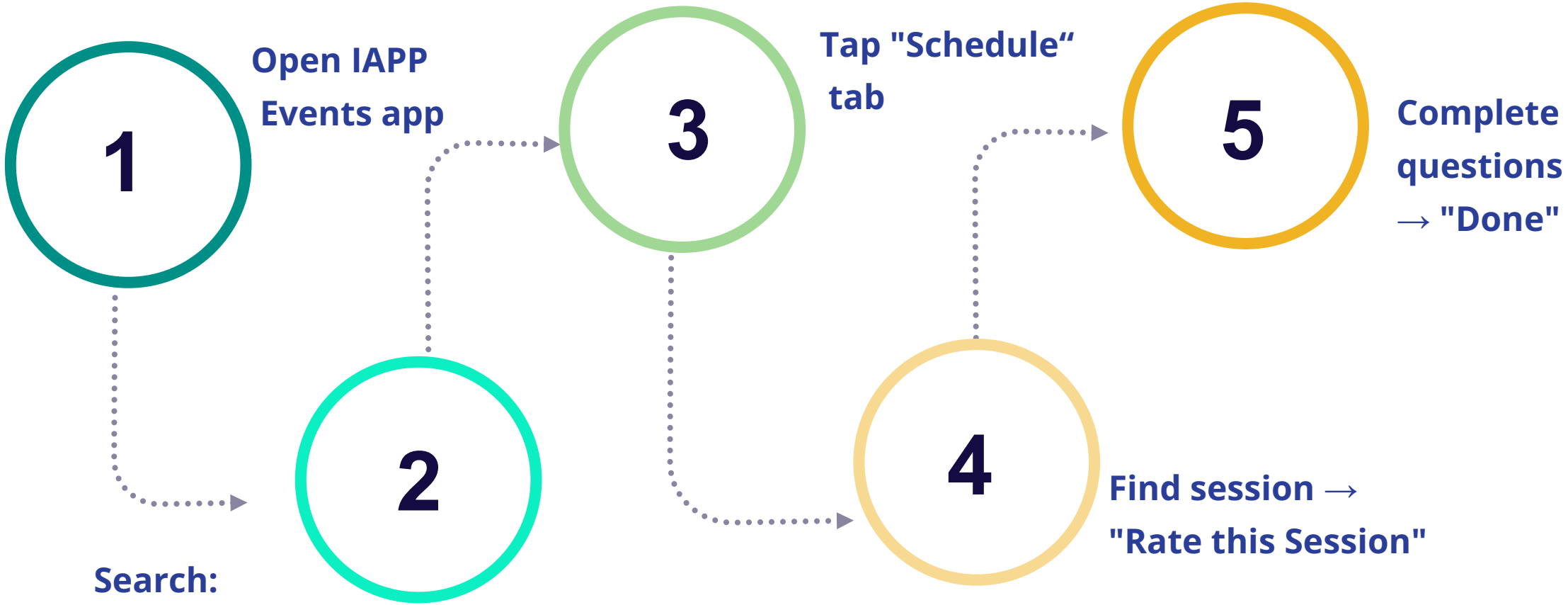
• NIST Cybersecurity Framework Roles and Responsibilities Overview
https://www.nist.gov/cyberframework

Post-Incident Evaluation Framework

Analysis tool for continuous improvement and lessons learned documentation

• NIST SP 800-61: Post-Incident Activity (Lessons Learned Section)
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf#page=67

How Did Things Go?
(We Really Want To Know)



Thank you!

#PSR25

How Did Things Go?
(We Really Want To Know)

Did you enjoy this session? Is there any way we could make it better? Let us know by filling out a speaker evaluation.

1. Open the IAPP Events app.
2. Select **IAPP Privacy. Security. Risk. 2025**
3. Tap "Schedule" on the bottom navigation bar.
4. Find this session. Click "Rate this Session" within the description.
5. Once you've answered all three questions, tap "Done".

Thank you!