Center for Internet Security

CITOC

# Court TTX

## Tabletop Exercise

## Court in Crisis: Phishing to Ransomware

CTC KANSAS CITY 2025

HOSTED BY NCSC National Center for State Courts

TLP:GREEN

# Learning Objectives

1) Participate in and understand the value of a facilitated tabletop exercise (TTX)
2) Assess your organization's preparedness, and identify gaps in internal controls, policies, and operational procedures that could impact court operations and confidence in courts during a cyber event.
3) Gain resources and knowledge to facilitate your own TTX's

# Scenario Team

Subtitle or summary

**Robert Adelardi**

CIO, Eleventh Judicial Circuit of Florida Administrative Office of the Courts (CITOC Board Member)

**Stephen Jensen**

Sr. Director of Plans, Programs & Exercises, Multi-State Information Sharing and Analysis Center (MS-ISAC), a division of the CIS

**Shay Cleary**

Managing Director, Technology Architecture Planning and Security, NCSC

**Jannet Okazaki**

Deputy Managing Director, Technology Architecture Planning and Security, NCSC

**Mariluz “Mari” Maldonado**

Senior Court Consultant and Planner, NCSC

# Cybersecurity and Incident Response is a Team Sport

# Important Notes

1) This session is providing a "taste" of what a tabletop (TTX) exercise is like
2) A TTX typically contains the following elements:
    1) Narrative (overall context of what's happening in the scenario)
        - Inject (new event, complexity or information)
    2) Problem Solving (discussion at table)
    3) Report Out & Discussion (how the team responded, what could have been done differently or better)
3) Parking lot (capture lessons learned that can be applied to your court)

# Important Notes (continued)

1) Actively participate in scenario
2) Actively respond to questions and debrief
3) Sometimes you will be asked to respond as a table, from the perspective of your court, or as your role in real life
4) Second workshop will be different scenario
5) Consider this TLP Green

# Traffic Light Protocol (TLP)

CISA (Cybersecurity and Infrastructure Security Agency) developed latest version of protocol to facilitate proper sharing/collaboration of sensitive information

- Five labels:
  - TLP:CLEAR – Safe for public dissemination
  - TLP:GREEN – Limited disclosure, can share within community
  - TLP:AMBER – Need-to-know within your org and client
    - TLP:AMBER + STRICT – Your organization only
  - TLP:RED – for your eyes only

# scenario

# Court in Crisis
# Phishing to Ransomware

# Court in Crisis

## Segment 1 – Alert Released

# Court in Crisis > Segment 1 > Alerts Released

**Day 1, Friday 8:00AM**

- The Department of Homeland Security (CISA) issues an alert on a new ransomware variant targeting SLTT governments.

**Day 4, Monday 10:00AM**

- The MS-ISAC follows with an alert on a phishing campaign tied to this ransomware. Emails disguised as HR updates or invoices contain malicious attachments.

# Court in Crisis > Segment 1 > Alerts Released

## Scenario

- **Monday 11:30AM (Day 4)**
  Two alerts have been issued regarding a new ransomware variant

## Discussion Questions (at your table)

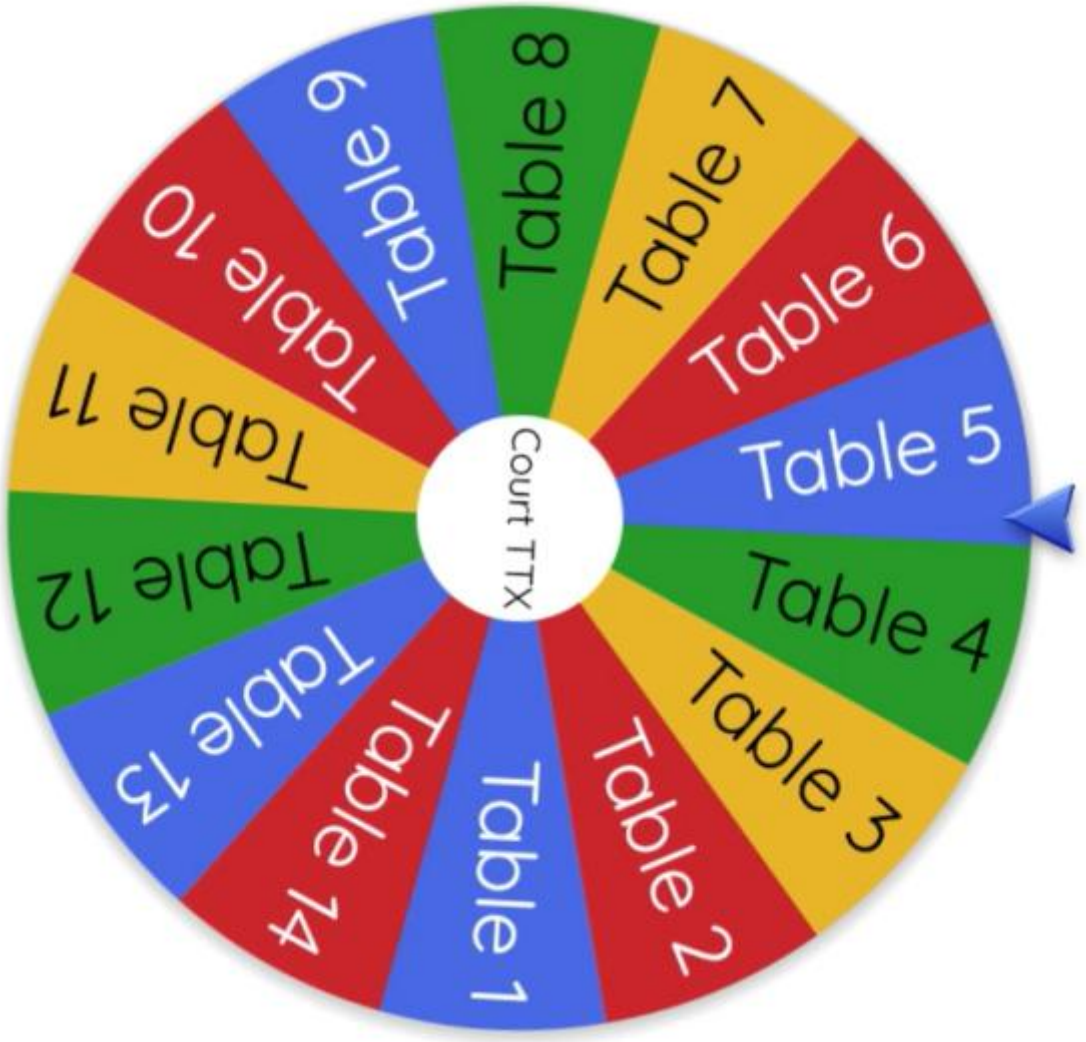
- How would your court realistically hear about alerts like this?
- Who sees the alerts first, and how is it shared?
- Would it be circulated beyond IT at this stage?

5:00

# Court in Crisis > Segment 1 > Random Report Out

## Discussion Questions

- How would your court realistically hear about alerts like this?
- Who sees the alerts first, and how is it shared?
- Would it be circulated beyond IT at this stage?



# Court in Crisis

## Segment 2 – Phishing Email Reported

# Court in Crisis > Segment 2 > Phishing Email Reported

**Day 5, Tuesday 10:00AM**

- A user forwards a suspicious email: Subject: “Updated HR Benefits Policy – Immediate Action Required.”
- The emails have an attachment and also a link.
- IT discovers similar emails were received by multiple users.

# Court in Crisis > Segment 2 > Phishing Email Reported

## Scenario

**Tuesday 10:00AM (Day 5)**
Confirmation of users receiving phishing email

**Monday 11:30AM (Day 4)**
Two alerts have been issued regarding a new ransomware variant

## Discussion Questions (at your table)

- What steps would be taken right now?
- Who would you notify, and how?
- Who decides if the incident response team should be activated?

5:00

# Court in Crisis > Segment 2 > Random Report Out

## Discussion Questions

- What steps would be taken right now?
- Who would you notify, and how?
- Who decides if the incident response team should be activated?

# Court in Crisis

## Segment 3 – Overnight Escalation

# Court in Crisis > Segment 3 > Overnight Escalation

**Day 6, Wednesday 1:00AM**

- Despite efforts to block the phishing campaign, a traveling user opens the email, provides credentials, and the malware spreads.
- Credentials are escalated and throughout the night databases and systems are encrypted.

**Day 6, Wednesday 7:00AM**

- By early morning CMS and most systems are down, including email.
- The only backups that can be accessed are two weeks old.

# Court in Crisis > Segment 3 > Overnight Escalation

## Scenario

- **Wednesday 8:00AM (Day 6)**
  CMS and most systems are down, including email. Can only access backups two weeks old.

- **Tuesday 10:00AM (Day 5)**
  Confirmation of users receiving phishing email

- **Monday 11:30AM (Day 4)**
  Two alerts have been issued regarding a new ransomware variant

## Discussion Questions (at your table)

- Who needs to be in the first meeting, and where/how do you meet?
- What do you tell staff and judges?
- What outside entities need to be notified?

5:00

# Court in Crisis > Segment 3 > Random Report Out

## Discussion Questions

- Who needs to be in the first meeting?
- Where/how do you meet?
- What do you tell staff and judges?
- What outside entities need to be notified?

# Court in Crisis

## Segment 4 – It Gets Worse

# Court in Crisis > Segment 4 > It Gets Worse

**Day 6, Wednesday 1:30PM**

- A ransom note appears on some computers: ‘Your files have been encrypted. Pay 15 Bitcoin in 72 hours or your data will be permanently encrypted’.

**Day 6, Wednesday 2:30PM**

- Social media posts claim data may have leaked.

**Day 6, Wednesday 2:45PM**

- Justice partners start severing connections to your court.

# Court in Crisis > Segment 4 > It Gets Worse

## Scenario

- **Wednesday 3:00PM (Day 6)**
  Confirmed ransomware, threat of data leak, justice partners disconnecting
- **Wednesday 8:00AM (Day 6)**
  CMS and most systems are down, including email. Backups two weeks old
- **Tuesday 10:00AM (Day 5)**
  Confirmation of users receiving phishing email

## Discussion Questions (at your table)

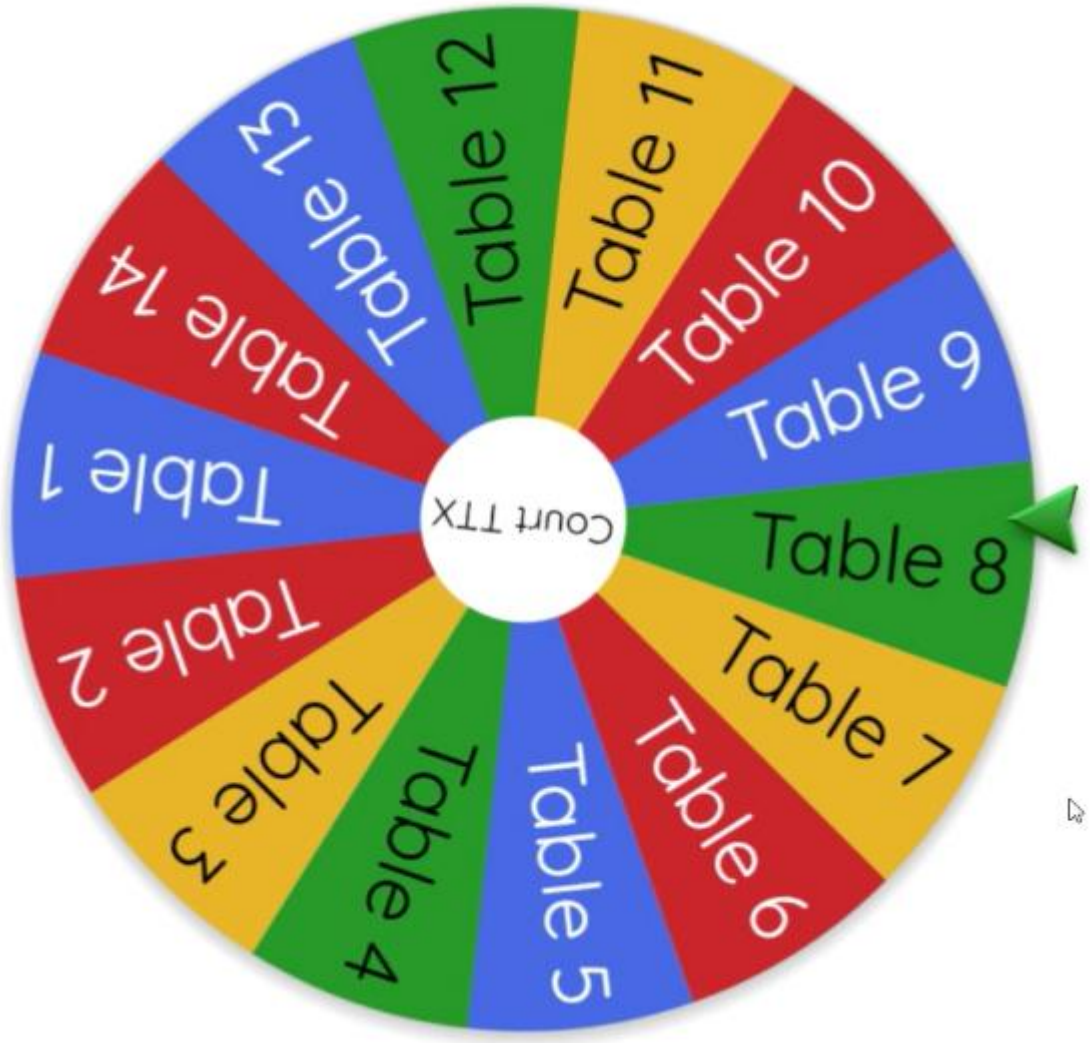
- What essential services do you prioritize?
- What do you communicate to justice partners?
- What do you tell the media/public about delays and leaked data?

5:00

# Court in Crisis > Segment 3 > Random Report Out

## Discussion Questions

- What essential services do you prioritize?
- What do you communicate to justice partners?
- What do you tell the media/public about delays and leaked data?



NCSC/JTC Court Virtual TTX October 2025 (open to ALL Courts)

Security For Justice Event CITOC May 2026

JTC Paper Cybersecurity Basics for Courts 2025

Reasonable Cybersecurity Guide (CIS Paper)

SJI Funded Cybersecurity Workshop Workbook

JTC Cybersecurity Incident Planning and Response for Courts 2025

# Thank you.