CIS. Center for Internet Security®

CITOC

Court TTX

Tabletop Exercise

Court in Crisis: Operation Tidalwave

CTC KANSAS CITY 2025

HOSTED BY NCSC National Center for State Courts

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
Operation Tidalwave

A Distributed Denial of Service attack on public facing Court systems impacting normal operations and public perception of the justice system.

Court in Crisis

Segment 1 – A Light Rain

Court in Crisis > Segment 1 > A Light Rain

Day 1, Monday 9:30AM

- It's a quiet Monday afternoon. The IT monitoring dashboard shows a modest spike in inbound traffic to the court's public-facing website. You have recently launched a campaign promoting online **services, so the uptick seems expected. But the SOC flags something odd—80% of the traffic is coming from Eastern Europe and Southeast Asia**, regions not typically associated with your user base.

Day 1, Monday 11:45AM

- The Cybersecurity and Infrastructure Security Agency (CISA) issues an alert: Hacktivist groups are threatening to disrupt services of regional government agencies within the next week. No specific targets are named.

Court in Crisis > Segment 1 > A Light Rain

Scenario

- **Monday 11:45AM (Day 1)** Spike in network traffic and an alert of targeted hacktivist activity

Discussion Questions (at your table)

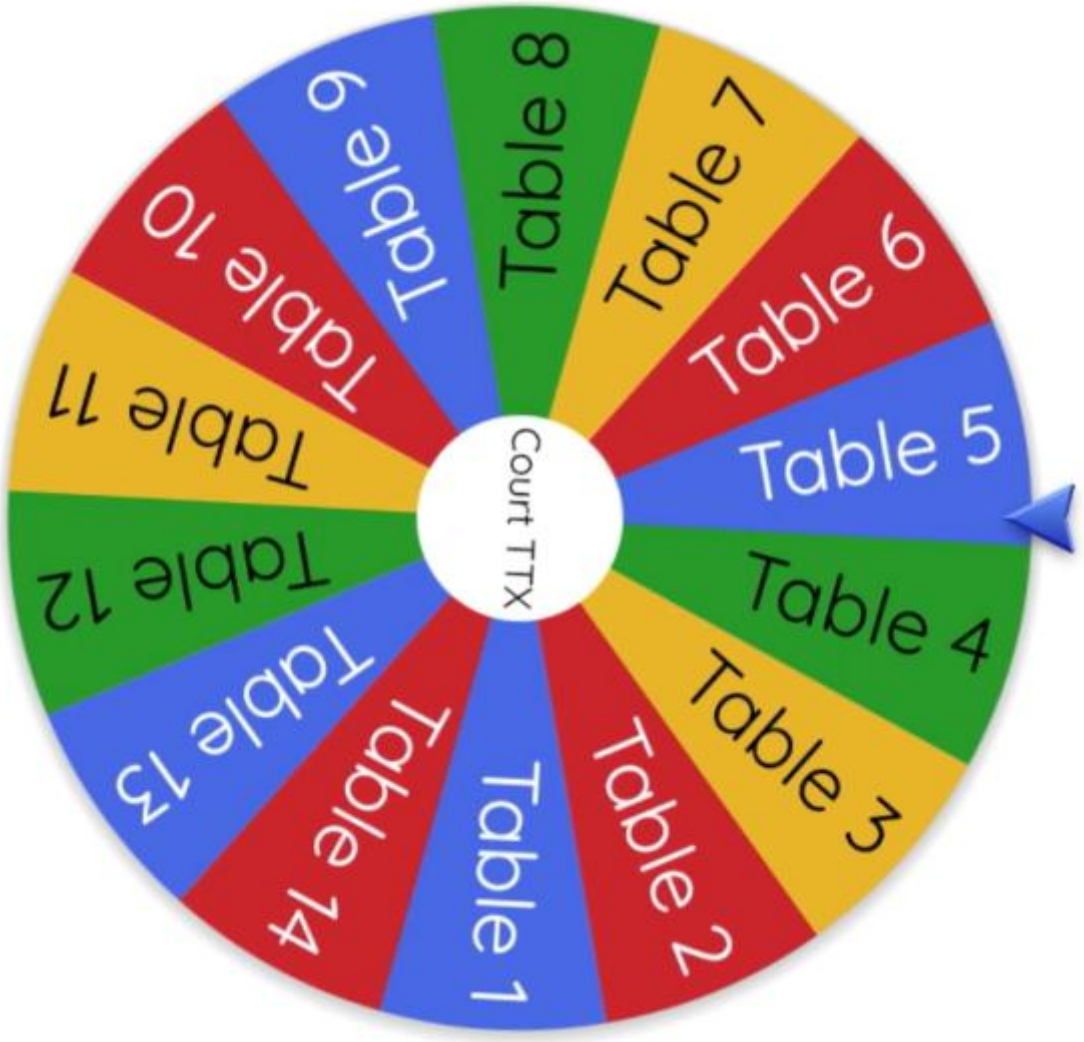
- Who does your organization receive real-time threat intelligence from?
- Does your IT team keep logs that can be used record as your current baseline for abnormal network activity?

5:00

Court in Crisis > Segment 1 > Random Report Out

Discussion Questions

- Who does your organization receive real-time threat intelligence from?
- Does your IT team keep logs that can be used record as your current baseline for abnormal network activity?



Court in Crisis

Segment 2 – A Light Rain Continued

Court in Crisis > Segment 2 > A Light Rain Continued

Day 1, Monday 2:30PM

- The help desk logs show sporadic reports: Users report that the court websites are either loading extremely slowly or not at all and that they are unable to log into e-filing and jury portals. The outages are brief and inconsistent but growing in frequency.

Day 1, Monday 2:35PM

- A network engineer notices a surge in login requests—**from 3,000/minute to over 60,000/minute**. The requests originate from dozens of countries. The pattern is unmistakable: **a distributed attack is underway**, targeting your public facing infrastructure.

Court in Crisis > Segment 2 > A Light Rain Continued

Scenario

Monday 3:00PM (Day 1)
Court websites and portals experiencing outages and login requests consistent with DDoS attack.

Monday 11:45AM (Day 1)
Spike in network traffic and an alert of targeted hacktivist activity

Discussion Questions (at your table)

- At what time during the events of the day does the situation become reportable beyond the IT department?
- Is there a trigger for when to perform this reporting?
- Who are key decision makers to gather immediately?

5:00

Court in Crisis > Segment 2 > Random Report Out

Discussion Questions

- At what time during the events of the day does the situation become reportable beyond the IT department?
- Is there a trigger for when to perform this reporting?
- Who are key decision makers to gather immediately?

Court in Crisis

Segment 3 – Weathering the Storm

Court in Crisis > Segment 3 > Weathering the Storm

Day 1, Monday 3:30PM

- Public facing systems are completely unavailable. Monitoring tools show inbound traffic peaking at 500,000 requests per minute, overwhelming upstream bandwidth. The attackers appear to be rotating the source IP addresses to sustain the pressure.
- Clerks, attorneys, and justice partners begin calling to confirm outages. Social media erupts with speculation. A trending hashtag claims the judiciary has been “hacked.” Reporters email and call your Public Information Office (PIO) for comment.
- A third-party vendor—whose systems are integrated with yours—reports they’re under attack too. They’re considering severing connections to protect their infrastructure.

Court in Crisis > Segment 3 > Weathering the Storm

Day 1, Monday 4:30PM

- Your ISP calls to report that they have begun instituting mitigation measures. Some of these measures involve “null-routing” attacker IP addresses while your local IT staff have begun configuring traffic filtering and geographic IP blocking

Day 2, Tuesday 8:00AM

- Although some services are restored, the courts E-File system and online public access systems are still offline. These systems allow attorneys to electronically file documents and allow the public to view information about a filled cases.

Court in Crisis > Segment 3 > Weathering the Storm

Scenario

- **Tuesday 8:30AM (Day 2)**
  While some of the attack has been mitigated, eFiling and public access still down. Trending social media reports courts hacked.

- **Monday 3:00PM (Day 1)**
  Court websites and portals experiencing outages and login requests consistent with DDoS attack.

Discussion Questions (at your table)

- What is your strategy for restoring critical services?
- Does this exceed your Court's ability to respond with your available IT resources?
- How do you document decisions for post-incident review?
- What communication (if any) are you sending internally and externally?

5:00

CTC KANSAS CITY 2025

HOSTED BY NCSC National Center for State Courts

TLP:GREEN

Court in Crisis > Segment 3 > Random Report Out

Discussion Questions

- What is your strategy for restoring critical services?
- Does this exceed your Court's ability to respond with your available IT resources?
- How do you document decisions for post-incident review?
- What communication (if any) are you sending internally and externally?

Court in Crisis

Segment 4 – The Flood Recedes

Court in Crisis > Segment 4 > The Flood Recedes

Day 3, Wednesday 8:00AM

- Most services are stable with the last few projected to be good to go by the end of the day. The attack has subsided, but the damage is done. Public trust is shaken. The judiciary must now assess its vulnerabilities and prepare for future threats.
- A post-incident review is scheduled. The Chief Justice wants a full report on what happened, how it was handled, and what will be done to prevent recurrence.

Court in Crisis > Segment 4 > It Gets Worse

Scenario

- **Wednesday 8:00AM (Day 3)** Services are stable, Chief Justice wants full post incident report.

- **Tuesday 8:30AM (Day 2)** While some of the attack has been mitigated, eFiling and public access still down. Trending social media reports courts hacked.

Discussion Questions (at your table)

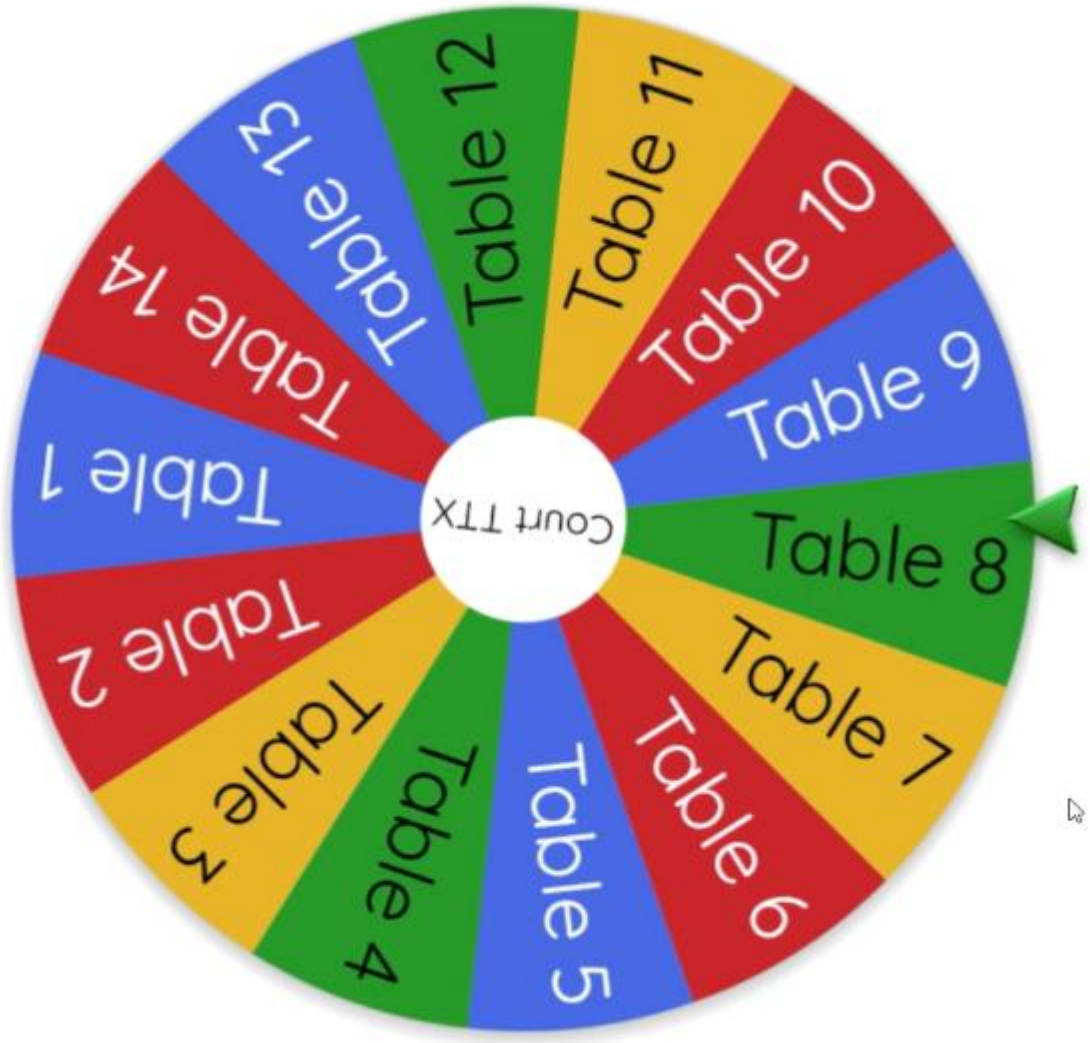
- What is your process for declaring recovery, and who authorizes that announcement?
- Do you report the incident to law enforcement?
- What are your key takeaways from the incident?

5:00

Court in Crisis > Segment 3 > Random Report Out

Discussion Questions

- What is your process for declaring recovery, and who authorizes that announcement?
- Do you report the incident to law enforcement?
- What are your key takeaways from the incident?



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.