2026 Regional Cybersecurity Workshop: Tabletop Exercise (TTX)

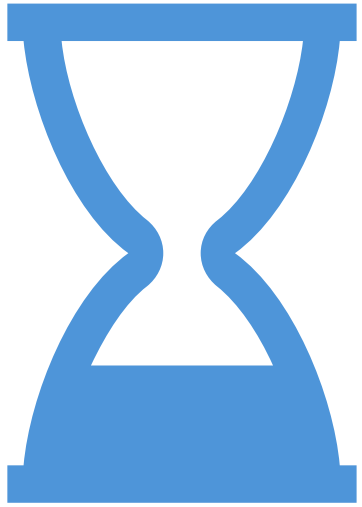
Learning Objectives

- Recognize and escalate cyber threats
- Execute initial incident response actions
- Maintain critical court operations during disruption
- Communicate effectively with internal and external stakeholders
- Navigate legal and policy decisions (including ransom considerations)
- Identify gaps in planning and improve preparedness

Important Notes

- This is a sample of a full-fledged, potentially multi-day tabletop exercise.
- Tabletop exercises normally consist of narrative with injections, problem solving, and reporting.
- The lessons learned from this exercise are more important than “successfully” completing it.
- Active engagement through discussions and responses will allow participants to get the most out of the exercise.
- Your grouping will be asked for responses for one or more questions.

Phase 1: Day 0 – Prior Afternoon (~ 4:00 PM)



- IT staff notice intermittent, unexplained activity on the network.
- A few employees report being briefly locked out of their accounts.
- IT logs show multiple failed login attempts from an unfamiliar external IP address.
- A clerk reports receiving a suspicious email earlier in the day with an attachment labeled “Updated Court Schedule,” but they are unsure if they opened it.
- At this point, IT begins investigating but does not escalate the issue, believing the behavior may be routine instability or user error.

Phase 1: Potential Questions & Discussion (10 Minutes)

- Would this trigger an incident or just additional monitoring?
- What tools or alerts should catch this?
- Is there a defined threshold for escalation or is it judgment-based?
- Who should be notified at this stage?
- Who has authority to initiate an incident response before impact is confirmed?

Phase 2: Day 1 – Systems Go Down (9:15 AM)

- Court staff begin reporting they cannot access files from their drive shares.
- Error messages begin to appear stating files are “corrupted.”
- Shortly after initial reports, all shared drives become inaccessible.
- At 9:30 AM, a ransom note appears on multiple screens: “Your files are encrypted. Pay 25 Bitcoin (~ $1.6 million) within 5 days or all data will be leaked and destroyed.”

Phase 2: Potential Questions & Discussion (10 Minutes)

- Who declares this a cyber incident?
- What are your first 3 actions (be specific)?
- Do you shut down systems?
- What internal communication method do you use if email is compromised or down?
- How do you operate court today (hearings, filings, payments)?

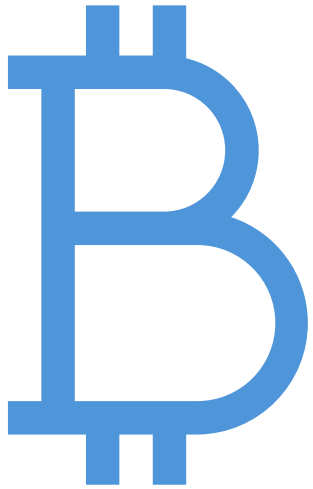
Phase 3: Day 1 - Escalation & Public Pressure (11:00 AM)

- Local media outlets are calling for information after seeing a social media post shared by an alarmed employee.
- A frustrated judge wants to proceed with hearings.
- IT suspects data may have been accessed and not just encrypted.
- Other county systems like may be affected.

Phase 3: Potential Questions & Discussion (10 Minutes)

- What information can you safely share vs. what should be withheld?
- How do you handle misinformation or rumors spreading online?
- What guidance do you give judges about proceeding vs. pausing cases?
- Who coordinates with law enforcement / state partners?
- How do you support staff who are overwhelmed or unsure what to do?

Phase 4: Ransom & Recovery Decision (1:00 PM)



- Attackers claim they will release sensitive data unless payment is received.
- Backups exist to restore systems, but the process will take ~1 week.
- County and court leadership are under pressure to restore quickly.

Phase 4: Potential Questions & Discussion (10 Minutes)

- What is your communication plan during a multi-day outage?
- Who makes that decision or is there a pre-existing policy on ransom payments?
- What are your legal and ethical considerations?
- What cases get prioritized during outage (e.g., criminal, protection orders)?
- How do you handle potential data breach notifications?

Final: Wrap-up Questions

- What single failure contributed most to this incident?
- How do you encourage transparency with the public?
- What decision was the hardest to make and why?
- What are your top three takeaways from this session?
- What questions do you have for other counties like you?

Contact Information

Wendy Hosch
Assistant Director of Information Technology
Administrative Office of Pennsylvania Courts
Wendy.Hosch@pacourts.us

Tyler Simmons
Cybersecurity Officer
Administrative Office of Pennsylvania Courts
Tyler.Simmons@pacourts.us