Practice Your Crisis

Wm. Bruce Wray
www.WrayLawTCP.com

Wm Bruce Wray
Owner / Managing Partner
Wray Law TCP

Boutique legal support with a global perspective for your technology, cybersecurity, and privacy needs.

www.wraylawtcp.com
https://www.linkedin.com/company/wraylawtcp

Tabletop Exercises (TTX)

1. Surviving A Security Firestorm, Being Prepared for Your Next Incident
    - ISC2 Omaha Lincoln Local Chapter Meeting
    - September 15, 2025
2. **Practice Your Crisis**
    - **NEbraskaCERT CSF**
    - **September 17, 2025**
3. Using TTX: How Not To Crisis Your Crisis
    - Nebraska Cyber Security Conference
    - September 29, 2025

Surviving A Security Firestorm, Being Prepared for Your Next Incident

Incident Response Lifecycle

- Preparation
- Detection and analysis
- Containment
- Eradication
- Recovery
- Post-incident activities

Roles and Responsibilities

- Building an Incident Response Team
  - IT Operations
  - Security
  - Legal
  - Communications
  - … but also Executives, Business Operations, Sales, Customer Service, Support, etc.
- Allocation of Roles and Responsibilities
- Understanding Conflicting Objectives

Practice Your Crisis

Practice Means Tabletop Exercises (TTX)

- Simulation-based drills
- Testing processes, not systems
- Safe environments to practice decision-making and communications

TTX Objectives

- Validate Incident Response Plans/Playbooks
- Clarify roles:
  - Operations, Security, Legal, Comms/PR, Execs, etc
- Test decision-making under pressure

BCP/DR vs IR TTX

- Normalization of BCP/DR TTX
- Need for Incident Response TTX

First Steps

- Create initial TTX task force
- Choose top-relevant incidents (e.g., phishing-ransomware hybrid)
- Schedule first TTX and follow-up actions

Structure

- Prepare
- Facilitate
- Debrief
- Implement Change

Prepare

Define:

- Scope
- Threat scenario
- Participants
- Materials

Facilitate

During:

- Use a designated moderator
- Run the scenario
- Replicate time pressures
- Simulate the external pressures

Debrief

Immediately after, identify:

- Gaps
- Assumptions
- Strengths
- Weaknesses
- Opportunities
- Threats

Implement Change

After the dust settles, plan for updates to:

- Policies
- Playbooks
- Registers
  - (i.e. risk registers, data registers, data movement registers, asset registers, resource registers)
- Communications Plans
- Contact Lists

Next Steps

As your TTX Maturity Model increases:

- Expand TTX task force with defined job descriptions
- Vary the top-relevant incidents
- Establish regular cadence for TTX action cycle

Measuring Success

- Define Metrics:
  - Plan coverage, decision time, communication clarity
- Track Improvements:
  - Speed, role clarity, communications, documentation updates

Lessons Learned & Actions

- Establish a regular cadence
  - Quarterly is recommended
  - Semi-Annual or Annual
- Keep scenarios evolving with new threats
  - Vary the tests, the scope, the participants
- Greater involvement from executives helps reinforce a cybersecurity aware culture

Using TTX: How Not To Crisis Your Crisis

Nebraska Cyber Security Conference
September 29, 2025

Q&A