Incident Response Tabletop Exercises

They're not just a game.

REN-ISAC

Who am I?

REN-ISAC

Shane Albright

REN-ISAC

- Principal Security Engineer
- 20 years of IT and infosec experience
  - 15 years in higher education
- CISSP, CCSP, 5x GIAC

What is a tabletop exercise?

REN-ISAC

Why bother?

- Improve incident response plan and related processes
- Improve incident response team collaboration and decision making
- Clarify roles and responsibilities during an incident
- Identify and contain incidents faster
- Reduce the cost of an incident
- Improve security awareness
- Prepare leadership for an incident

Are you exercising your IR plans?

Planning

REN-ISAC

Questions to Answer

- Who from the executive level is providing support?
- What are your organization's objectives for the tabletop exercise?
  - What benefit do you hope to gain?
  - What would your organization like to learn from this tabletop exercise?
  - Is it being performed to meet a contractual or compliance obligation?
- Whom should you invite to participate?
- What logistics are involved and who's handling them?

Executive Sponsor’s Responsibilities

- Announce the exercise
- Attend the kickoff planning meeting
- Attend the exercise and participate

Potential Objectives

- Rehearse the incident response plan
- Understand organizational roles and responsibilities during an incident
- Understand vendor roles and responsibilities during an incident
- Evaluate communications processes during and after an incident
- Identify areas of improvement in your incident response plan and overall organizational resilience
- Ensure strategic alignment across leadership in addressing incidents

Senior Level vs. Operational Level

Who should participate?

- Information Technology
- Information Security
- Emergency Operations
- Risk Management
- Legal Counsel
- Finance
- Human Resources
- Public Relations / Communications
- Campus Safety / Law Enforcement
- Purchasing / Procurement
- Service Providers

Roles

- Participants
- Observers
- Facilitator(s)
- Note Taker(s)
- Evaluator(s)

Logistical Considerations

- In-Person vs. Remote
- Duration
- Date and Time
- Location

Scenario Development

REN-ISAC

Inspiration

- A recent incident at your institution
- A recent incident in the news
- A known risk to your institution
- An episode of Darknet Diaries

Exercise Structure

The Six Stages of Incident Response (PICERL)

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

Exercise Structure

NIST SP 800-61 Incident Response Life Cycle

1. Preparation
2. Detection & Analysis
3. Containment, Eradication, and Recovery
4. Post-Incident Activity

Exercise Structure

Cyber Kill Chain®

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control
7. Actions on Objectives

What's an inject?

Creating the Scenario

- Tell a story
- Direct the focus of the exercise
- Allow attendees to explore a variety of topics
- Start with an outline
- Use Backdoors & Breaches or the MITRE ATT&CK framework for inspiration

Example Scenarios

- Ransomware
- Cloud Account Takeover
- Business Email Compromise
- Insider Threat
- Cloud Vendor Compromise / Outage
- Building Automation System Compromise
- ePHI Data Breach

Planning the Agenda

- Introductions
- Threat Briefing (Optional)
- Preamble
- Injects and Questions
- Debrief and Q&A

Slides and Handout

- Introductions
- Threat Briefing (Optional)
- Preamble
- Injects and Questions
- Debrief and Q&A

Facilitation

REN-ISAC

The Facilitator's Role

- Present the scenario and injects
- Guide the discussion
- Provide clarification, when needed
- Ask targeted questions
- Identify comments or concerns that warrant further discussion
- Keep track of the time and move the exercise along

Preparation

- Compile a list of questions
- Assign the role of scribe or note-taker
- Consider recording the exercise

During the Exercise

Do:

- Be respectful and professional
- Think out loud and encourage participants to do the same
- Ask clarifying questions
- Intervene only when necessary

During the Exercise

Don’t:

- Don't let one or two people dominate the conversation
- Don't ask yes or no questions
- Don't ask leading questions

After the Exercise

- Survey attendees

Evaluation

REN-ISAC

The Evaluator's Role

- Review any recordings or notes
- Compile a list of findings and recommendations
- Write the after-action report

Methods of Evaluation

- Review recording
- Review note taker's notes
- Debrief attendees
- Survey attendees

Deliverables

REN-ISAC

Statement of Completion

- Date and Time, Location, Duration
- List of Attendees
- Brief Description of Scenario

After-Action Report

- Executive Summary
- Description of Scenario
- Findings and Recommendations

Follow-Up Activities

REN-ISAC

Follow-Up Activities

- Update your incident response plan
- Organize and update other documentation
- Conduct follow-up exercises
- Create a formal tabletop exercise program
- Present the high-level findings, recommendations, and follow-up activities to leadership

Resources

REN-ISAC

Resources

- *Cybersecurity Tabletop Exercises* by Robert Lelewski and John Hollenberger
- *Backdoors & Breaches*
- CISA Tabletop Exercise Packages (CTEP)
- MITRE ATT&CK
- Generative AI

REN-ISAC's Offerings

REN-ISAC

Tabletop Exercises

REN-ISAC Information Security Assessment & Advisory Services

- Three Tiers
  - General Scenario with Statement of Completion
  - Custom Scenario with Statement of Completion
  - Custom Scenario with Statement of Completion and After-Action Report
- 3–4 Hours
- On-site or Remote

Questions

REN-ISAC

Contact Information

REN-ISAC Information Security Assessment & Advisory Services

Kyle Enlow, Program Manager

peer@ren-isac.net

+1 (812) 855-8739

Shane Albright, Security Advisor

saalbrig@ren-isac.net

+1 (812) 856-6071

https://www.ren-isac.net/ISAAS