OmniSOC

The Higher Education & Research
Security Operations Center

What is a cyber incident drill?

- A type of security exercise - A structured simulation that tests how well people, processes, and systems respond to a security incident under realistic conditions.
- So...like a tabletop exercise?

Cyber incident drills are like cybersecurity fire drills

- A cyber incident drill includes key live elements that go beyond discussion:
    - Simulate initial discovery of an incident
    - Practice real communications between stakeholders
    - Added steps relevant to the scenario and your goals

Why should I do cyber incident drills?

- They build readiness.
- They test assumptions and reveal weaknesses in procedures
- They confirm critical tools and failover processes work when needed
- They create elasticity in thinking.
- Bonus: Drills can also help meet IMO Cyber Risk Management requirements.

How do I conduct a cyber incident drill?

- Cyber incident drills primarily have 3 phases:
  - Planning
  - Execution
  - Follow-up

Planning

- Define the goal — what are you testing or validating?
- Choose a realistic scenario and scope.
- Identify people, systems, and procedures involved.
- Outline assumptions you want to test.
- Set success criteria — what does “good” look like?

Execution

- Notify necessary stakeholders ahead of time.
- Assign and brief participants (**facilitator, note taker, “players”, “NPCs”, observers**).
- If necessary, communicate the scenario and its boundaries.
- Keep it realistic but controlled and safe
- Observe and capture what happens in real time.

Execution - Facilitation tips

- Have a clear start and end point – and identify key decision points along the way.
- Anticipate that plans will go off-script.
- Keep participants engaged and thinking.
- Capture key moments and decisions.

Follow-up

- Hold a debrief/post-mortem discussion immediately after the drill.
- Recap what happened — what worked and what didn't.
- Collect input from all participants and observers.
- Document observations and recommendations in a short report.

Building a cyber incident drill program - why?

- A program builds resilience.
- Iteration reinforces good behaviors and corrects weak ones.
- Regular drills turn rare, stressful events into routine problems to solve.
- Programs establish coordination and communication expectations across teams.
- Bonus again: Supports IMO Cyber Risk Management requirements.

Building a cyber incident drill program - how?

- Integrate lessons from completed drills into policies, pro
- Conduct drills on a regular cadence.
- Re-test areas improved since the last drill.
- Evolve scope and complexity over time.
- Track results and measure improvement.

Want help with a drill? Let us know

- The ARFSEC team can help you design and conduct a cyber incident response drill.

- Recently the ARFSEC team helped a fleet member with a drill. We planned out the scenario, provided and configured the necessary equipment to simulate an incident, and facilitated the drill. The drill took a few hours during a transit cruise.

OmniSOC

Thank you for your attention.

Questions?

omnisoc.iu.edu

@ arfsec@iu.edu

OmniSOC

omnisoc.iu.edu