OmniSOC

The Higher Education & Research
Security Operations Center

Cyber-incident Drill

Designing, executing, and maximizing the value of cyber-incident drills on your vessel.

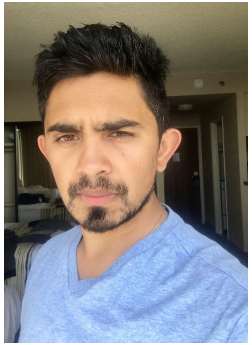
RVTEC 2024 - New Hampshire

Mike Simpson, Mikeal Jones, Chris Lauderbaugh, Vishal Bhardvaj and Ishan Abhinit

Introducing our team:

Mike Simpson

Mikeal Jones



Ishan Abhinit

Vishal Bhardvaj

Chris Lauderbaugh

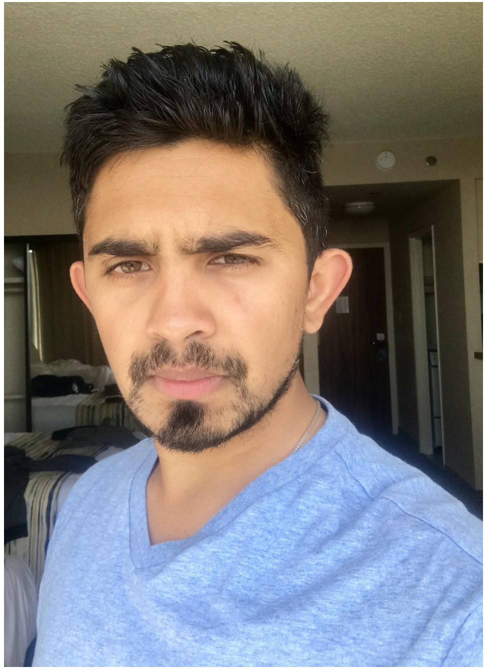
Mike Simpson

- **CISO for ARF**
- Senior Security Analyst at OmniSOC
- 20+ years of experience in IT / Cybersecurity
- Areas of expertise:
  - Cybersecurity Program Development & Strategy
  - Network Security
  - Digital Forensics
  - Network Penetration Testing
  - Physical Security

Mikeal Jones

- **Leads CRMP / Compliance Documentation initiative**
- Security Analyst at OmniSOC
- 20+ years of experience in IT / Cybersecurity
- Areas of expertise:
  - IT Operational Strategy
  - Cybersecurity
  - Systems Architect + Admin

Ishan Abhinit



- **Leads Incident Response policy and procedures initiative**
- Senior Security Analyst at IU CACR
- 12+ years of experience in IT
- Masters degree in Cybersecurity
- Areas of expertise:
  - Cybersecurity Program Development & Strategy
  - Security Log Analysis

Vishal Bhardvaj

- Security Analyst at OmniSOC
- 10+ years of experience in IT
- Master of Science in Cybersecurity
- Areas of expertise:
    - Windows software development
    - Macintosh data recovery
    - Telecommunications (2G, 3G, 4G)

Chris Lauderbaugh

- Security Analyst at OmniSOC
- 10+ years of experience in IT/Cybersecurity
- Worked in the medical and defense industries before joining OmniSOC
- Areas of expertise:
  - Digital Forensics
  - Cybersecurity Intelligence

TOTALLY SAFE LINK & QR CODE

Link to RVTEC presentation folder with slides and useful files:

https://go.iu.edu/8rkm

Definitions:

- Security Exercises:
    - An exercise or drill designed to test or discover information about how policies, procedures, systems and resources function under simulated real-world circumstances.
        - Tabletop Exercise
            - Walk through of a hypothetical real-world situation for testing policies, procedures and resources.
        - Live Exercise
            - Exercise conducted using real systems and resources. Higher risk, but proves procedures work as intended.

Definitions:

- Our definition of Cyber-Incident drill:
    - A tabletop exercise with key live elements
    - Recommended live elements:
        - Initial discovery
        - Communications between key stakeholders
        - Others depending on the exercise’s focus or goals

Benefits of conducting Cyber-Incident Drills:

- High ROI - time required to run exercises is a great investment towards good responses to real incidents.
- Decisions are made on assumptions; exercises test those assumptions revealing how much truth or falseness is behind them.
- Find gaps or inaccuracies in policies and procedures.
- Build 'muscle memory' with IR procedures

Training Agenda

- Getting Started - Policy
- Designing and Building Exercises
- Executing the scenario
- Debrief, Reports, Findings & Recommendations
- BREAK

- Introduction to Example Scenario
- Example Scenario
- Debrief for Example
- Goodbye!

Getting Started - Policies

- Master Information Security Policy and Procedure (MISPP)
  - Represents core information security policies
  - States Mission and scope of cybersec program
  - Roles and responsibilities such as CISO, DCISO, Cybersec lead
  - Reference to other policies
  - Align with TCIF

Trusted CI Framework

- Trusted CI Framework
  - Minimum standard for a cybersec program.
  - Structured on 4 pillars -
    - **Mission alignment** - Mission Focus, Information Assets
    - **Governance**: Leadership, Risk Acceptance, Policy
    - **Resources**: Personnel, Budget
    - **Controls**: Baseline control set
  - Built around 16 Musts

CIS - Baseline Control Set

- TCIF's Must #15 talks about baseline control set
- Provides a foundation from which an org can pick their controls based on mission needs.
- All organizations must adopt one.
- We recommend CIS Baseline Control
  - 3 Implementation Groups with 158 safeguards in CIS v8
  - Start with IG1. IG2 builds upon IG1 and IG3 provides
  - CIS Control Navigator

Incident Response Policy and Procedure

- Outlines actionable steps
- Lays out
  - Scope and Goals
  - Roles and responsibilities
  - Communication/Reporting requirements
  - Pre & Post Incident activities
  - Specific scenarios
- Stages of Incident response:
  - Preparation
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Lesson learned

Cyber Risk Management Plan

- Requirement by IMO
- Combination of 2 amendments made to ISM Code
  - MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems
    - SMS is collection of policies, procedures, and guidelines that allow ships to operate safely and meet the requirements in ISM code.
  - MSC-FAL.1/Circ.3 - Guidelines on Maritime Cyber Risk Management
    - Per the document, "**cyber risk management means the process of identifying, analysing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level**" with the goal of "support[ing] safe and secure shipping, which is operationally resilient to cyber risks."
    - Functional Requirements: Identify, Protect, Detect, Respond, Recover

Build the exercise program

What is a security exercise

A **tool** to help us find and correct **errant assumptions** about our organization's security.

- Helps us to get better at dealing with things that (hopefully) rarely happen.
- Tells us if our policies are effective.
- Reveals the assumptions we have made that don't line up with reality.
- Creates elasticity in our thinking about how we respond to problems.

What causes failure?

How can improve our detection and response systems to address the issues most likely to cause loss of confidentiality, integrity or access to our data?

- **Missing Information**
  Comprehensiveness, Rigor, Opportunity
- **Multiple concurrent problems**
  Compartmentation, Fault Tolerance,
- **Inability to Detect or Respond**
  Opportunity, Rigor
- **Incorrect Information**
  Rigor, Comprehensiveness.

Beware of false knowledge; it is more dangerous than ignorance.

-George Bernard Shaw

Incorrect Information

What “facts” do we know about our organization but haven’t tested?

- How have updates changed the operation of security controls?
- What processes or tools are we relying on that we haven’t tested?
- What errors in reasoning exist in written policy/procedure that we aren’t aware of?
- Do our policies align with the goals and priorities of the rest of the org?

How do we find out?

Security Exercise *Programs*

A ***series*** of security exercises we run to continually ***improve*** our policies and processes and prepare our team for responding to real issues.

- It is ***iterative***.
- It ***reinforces*** good response behaviors and ***corrects*** bad response behaviors.
- Changes, ***stressful, rare events*** into ***routine problems*** to be handled.
- Establishes expectations for ***coordination*** and ***communication*** within and among teams.

Prerequisites

- What are you protecting and why?
  - Inventory
  - Priorities
- How are you going to achieve those goals?
  - Policies
  - Procedures
- Who will do what during and incident?
  - Defined responsibilities
  - Assigned to the role, not the individual

These can be simple documents, the important thing is that they exist as a starting point for iterating on your program.

“We will ensure data integrity while ensuring maximum availability for our researchers”

“During an incident the CISO will be authorized to…”

Elements of a successful program

- **Regularity**

  Exercises should be regular, repeatable, scalable and adaptable

- **Purpose and Focus**

  Exercises should have a clear focus that is tailored for your organization

- **Preparation**

  Exercises should be scheduled in advance, planned, and clearly communicated

- **Follow Through**

  Knowledge gained in exercises should be reviewed and applied regularly

Regularity

Just like any exercise program, repetition is essential. You might feel good about holding an exercise, but the benefit quickly disappears.

- Frequency should be scaled to the organization, from quarterly to nearly continuously
- Schedule in advance with regular intervals
- Don’t schedule around key absences, real events won’t consult the calendar and role alternates need practice as well

Purpose

Start from your organization's mission statement, what are your priorities and what are the most likely ways they could be threatened?

- Test for known vulnerabilities/threats you assume you have mitigated
- Utilize threat intelligence to ensure you have mitigated known threats
- What changes have been made in the environment recently? Are they working as expected?
- Keep in mind this process is evaluative and not assessing performance, they goal is to learn something to improve ***future*** performance.

Preparation

Plan the program in advance, and think about long term goals. Consider your resources, strengths and weaknesses when developing exercises.

- Set a schedule and stick to it, a simple exercise is better than doing nothing
- Start with the low hanging fruit; small, low impact exercises
- Increase the scope and challenge of exercises as your ability to respond improves.
- If you aren’t failing some of the time you aren’t making them challenging enough

Follow Through

Collecting, distilling, and applying the knowledge gained during each exercise is the most essential part.

- Treat every exercise as a success as long as something was learned
- Hold a debrief as soon after the exercise as possible including as many people involved as possible
- Create a report with a list of actionable recommendations and revisit the reports regularly
- Implement the recommendations or document why they cannot be implemented

> “Knowledge is of no value unless you put it into practice.”
>
> -Anton Chekhov

Types of Exercises

Tabletop Exercise

Real-time exercise where each role walks through a hypothetical event together

- Useful for streamlining policies and procedures
- Easy to run, requires few resources
- Does not test real systems as well as Live Exercises

Live Exercises

Real-time exercise run on test or production environments with at least two teams

- More realistic than a tabletop exercise, tests real or simulated equipment
- Requires more preparation and engagement than a tabletop exercise
- Requires a test environment or willingness to compromise production environment

Tabletop Exercises

Method

A moderator creates a scenario and runs the participants through it, much like a tabletop RPG. “What do you do?”

Requirements

- Moderator and a pre-written scenario
- Means of communicating in real time.
- Means of note taking and sharing at debrief
- Defined roles and responsibilities for participants

Drawbacks

- Less engaging
- May not adequately draw attention to inaccurate suppositions.

Live Exercises

Method

Two teams conduct live environment exercises on test or production hardware. Can be run as White team v Blue team or Red team v Blue team

Requirements

- Two teams of participants, (White/Blue, Red/Blue)
- Production or test environment
- Defined expectations and boundaries
- Means of note taking and sharing at debrief

Drawbacks

- Requires more resources/planning
- Confining exercise to specific test cases can be difficult
- Has potential to affect production

Let’s make an exercise

- Pick a relevant topic from the handout
  - What threats are relevant to my org?
  - What vulnerabilities do I think are covered?

- Make a list of resources required to test?
  - People
  - Documentation
  - Systems
  - Time

Create a scenario outline to serve as the template for the hypothetical response.

For the live aspects of the exercise create a set of parameters for the them. What are the objects, scope, and end conditions of the test.

Let’s make an exercise

- Description - a brief overview of the exercise to give to the participants
- What process/idea do you want to test?
- What assumptions about this process/idea are we making?

For tabletop aspects of the scenario decide how you will present information to the participants and get them thinking critically.

For live aspects of the scenario think about how you can focus the objectives around the systems and assumptions you want to test.

Let’s make an exercise

- Find the file ResearchersTargetedRansomware
- Let’s walk through this example exercise.
- You are feel to use this, or base exercises off it.

- What are the goals?
- What are the live elements?

RVTEC Presentation folder: https://go.iu.edu/8rkm

https://drive.google.com/drive/folders/1z3FLGmPqq5MgH95-nn1s3vJN4PS3a3YP

Executing the Scenario

- Assign Roles
  - Facilitator
  - Note Taker
  - Set Roles based on Disaster Recovery Plan
  - Any Additional Roles (NPCs)

Executing the Scenario

- Facilitator
  - Oversees the scenario. Provides the information that makes up the scenario and any twists along the way
- Note Taker
  - Records who, what, when, and how of the incident and the response. Does not take part in the exercise

Executing the Scenario

- Set Roles based on Disaster Recovery Plan
  - These are usually the roles that the individuals perform daily. If that isn’t possible, roles can be assigned
- Any Additional Roles (NPCs)
  - These people have knowledge of events that will happen and therefore do not play an assigned response role. Their job is to add to the scenario as needed or to observe.

Being a Good Facilitator

- Have a plan
    - Know where the scenario will start and end
    - Have an idea of how you will get from A to B.
- Expect the plan to go off the rails
    - Understand that the participants will throw curveballs your way
    - You cannot plan for everything
- Be prepared to toss the plan
    - You will not have to toss the whole plan, but you will have to improvise at some points
    - Be prepared to make adjustments as you go

Example (LARP)

- LARP - Live Action Role-Playing
  - Participants portray roles in a scenario designed and coordinated by a gamemaster or facilitator
  - “Gaming” vs. Professional scenarios
  - Essential elements
    - Setting
    - Props
    - Participants

Locations and Props

- Engine Room
- Bridge
- IT Office
- Server Room

Roles

- Gamemaster/Storyteller/Facilitator
  - Chris and Vishal
- Marine Technician
- IT Tech
- Chief Engineer
- Additional Engineer
- Captain
- Shore contact
- Others as needed

Debrief

Post-Exercise Activities

- Debrief/Post-Mortem Discussion
- Report
- Act
- Repeat

Post-Exercise Activities

Debrief/Post-Mortem Discussion

- When? - Immediately Following the Exercise
- Recap the Timeline of Events
- What Went Well?
- What Could Be Improved?

Post-Exercise Activities

Report

- Brief
- Readable - Narrative Format and Non-Technical.
- Format:
  - Executive Summary
  - Methodology
  - Findings & Recommendations
    - Actionable - Clear Steps to Improve Operations and Response.
  - Conclusion

Post-Exercise Activities

Act

- Plan and Implement Improvements
- Update Policies, Procedures and Playbooks
- Review and Supplement Staff/User Training

Post-Exercise Activities

Repeat - Build Momentum and Drive Maturity

- Exercises must be done at regular intervals to be most effective.
- Exercises should build on each other, evolve over time, remain challenging.

Beginning the Adventure

OmniSOC

Thank you for your attention.

Questions?

omnisoc.iu.edu

@ arfsec@iu.edu

OmniSOC

omnisoc.iu.edu