CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Conducting Cyber Exercises at the National Level

Key Message: Scenario-based exercises help organizations, governments, and nations prepare for, identify, and mitigate cyber risks.

Executive Summary

"Exercises allow national homeland security and emergency management personnel, from first responders to senior officials, to train and practice prevention, protection, response, and recovery capabilities in a realistic but risk-free environment. Exercises are also a valuable tool for assessing and improving performance, while demonstrating community resolve to prepare for major incidents." In addition, exercises help participating organizations "obtain objective assessments of their capabilities so that gaps, deficiencies, and vulnerabilities are identified and remedied prior to a real incident" [1].

In this podcast, Brett Lambo, Director of the Cyber Exercise Program with the U.S. Department of Homeland Security (DHS), discusses the use of cyber exercises to identify and mitigate cyber and IT infrastructure risks at the state, regional, federal, and international levels. Brett describes six types of discussion- and operations-based exercises as well as Cyber Storm, a full-scale national exercise. Brett is joined by Matt Butkovic, a member of the Resilience Enterprise Management team at CERT.

PART 1: OBJECTIVE, MOTIVATION, AND GETTING EVERYONE ON THE SAME PAGE

Purpose and Value of Cyber Exercises

Cyber exercises are used to

- create a no-fault environment for people to road test their cyber security and incident response plans and procedures
- determine how much they actually have in place
- ensure coordination paths work as intended
- step through procedures to expose gaps and redundancies
- build trust relationships with key stakeholders in advance of an actual incident
- have some fun without the associated risks of a real incident

Key Participants and Stakeholders

The key players in a cyber exercise are determined based on exercise objectives. They may include

- private-sector owners and operators of national infrastructures (analogous to the primary first-responders). These include owners and operators of internet-based networks and other public networks.
    - The U.S. DHS National Infrastructure Protection Plan identifies 18 critical infrastructure sectors.
- those involved in day-to-day network and system monitoring (patching and hardening systems, mitigating security risks)
- policy makers
- public affairs officials
- emergency managers
- law enforcement
- intelligence agencies

Getting Participants on the Same Page

Most people participate voluntarily. They understand the magnitude and the mission. Each exercise provides an opportunity to better understand the broader implications at a policy or national security level.

People generally understand their role but comprehensive understanding and an ability to execute their responsibilities only occur when working collectively to mount a good defense to a major cyber event.

Most events do not suffer from lack of participant interest.

PART 2: DISCUSSION- AND OPERATIONS-BASED EXERCISES

Discussion-Based Exercises

These include (typically conducted in this order)

- seminars or workshops: used as an educational forum to teach people what they need to know
- tabletop exercises: the most common form of discussion-based exercise, where people sit around a table and act out a fictional or simulated scenario.
- games: add an element of fun by playing out “what-if” alternatives and going beyond the articulated plan

Discussion-based exercises can be used to build relationships and create procedures where none exist by stepping through example scenarios.

Tabletop exercises can be used to validate procedures.

Operations-Based Exercises

These include (typically conducted in this order)

- drills
- functional exercises
- full-scale exercises

In drills and functional exercises, participants are responsible for responding, getting real-time information, doing real-time information sharing, performing as they would in a live incident, and watching how everyone responds as the exercise progresses.

A full-scale exercise typically is the same, just bigger in terms of magnitude, scope, and number of participants.

Selecting an Appropriate Type of Exercise

Exercise selection depends on

- the exercise objective such as creating a “burning platform” for continued collaboration and setting a baseline or watermark for future improvement (which is more in keeping with a discussion-based exercise)
- the maturity of the participating organization or community. For example, a full-scale exercise is not appropriate for a community that does not have well-developed procedures.

The primary purpose of most exercises is to build capacity. Smaller-scale exercises help senior leadership better understand the magnitude of cyber risks and vulnerabilities.

PART 3: CYBER STORM: A FULL-SCALE NATIONAL EXERCISE

Background

Three Cyber Storm exercises have been conducted, the most recent one in September 2010. Cyber Storm is a large-scale, national-level cyber exercise involving the private and public sectors. The objective is to determine how well the United States can navigate the response to a significant cyber event. The scenario reflects today's realities on the internet and is sufficiently technically sophisticated to challenge skilled participants.

Cyber Storm III was conducted using a draft of the National Cyber Incident Response Plan, which was critical in defining procedures, roles, responsibilities, and authority.

Lessons Learned and Next Steps

A typical question after each Cyber Storm exercise (2006, 2008, 2010) is "Did you fix it? Did you fix the problems you learned about?" This is not really the right question. Over the course of Cyber Storms I-III, the national capability has evolved. Cyber Storm has demonstrated a growing national capability to defend against and mitigate the effects of a large-scale cyber incident.

Each exercise confirms the need

- to share information
- to work collaboratively
- for intergovernmental and public-private-sector coordination

Each exercise addresses the following questions

- How well do we do what we say we want to do?
- Are the plans and procedures directionally and conceptually sound?
- Have we course-corrected and made desired improvements since the last exercise?

Plans for future Cyber Storm exercises are still in discussion and development. The U.S. Federal Emergency Management Agency (FEMA) has the responsibility for top-level national exercises.

Role of CERT

CERT assists DHS cyber exercise efforts in the following areas:

- developing credible, realistic cyber scenarios
- developing tools for improving and ensuring repeatability of cyber exercises
- designing processes and methods to define cyber exercise objectives
- equipping cyber exercise owners with tools to conduct the cyber exercise
- translating lessons learned from cyber exercises into improvement actions

Guidance is documented in the CERT report "Enhanced Methods for Cyber Exercise." (A link to this report will be added when it becomes available.)

Resources

[1] U.S. DHS Homeland Security Exercise and Evaluation Program

U.S. DHS Cyber Storm; Securing Cyber Space website

U.S. DHS National Cyber Security Division Cyber Exercise Program

U.S. DHS National Cyber Security Division website

U.S. DHS National Cyber Security and Communications Integration Center

US-CERT website

CERT website

CERT Podcast: Better Incident Response through Scenario Based Training (February 2009)