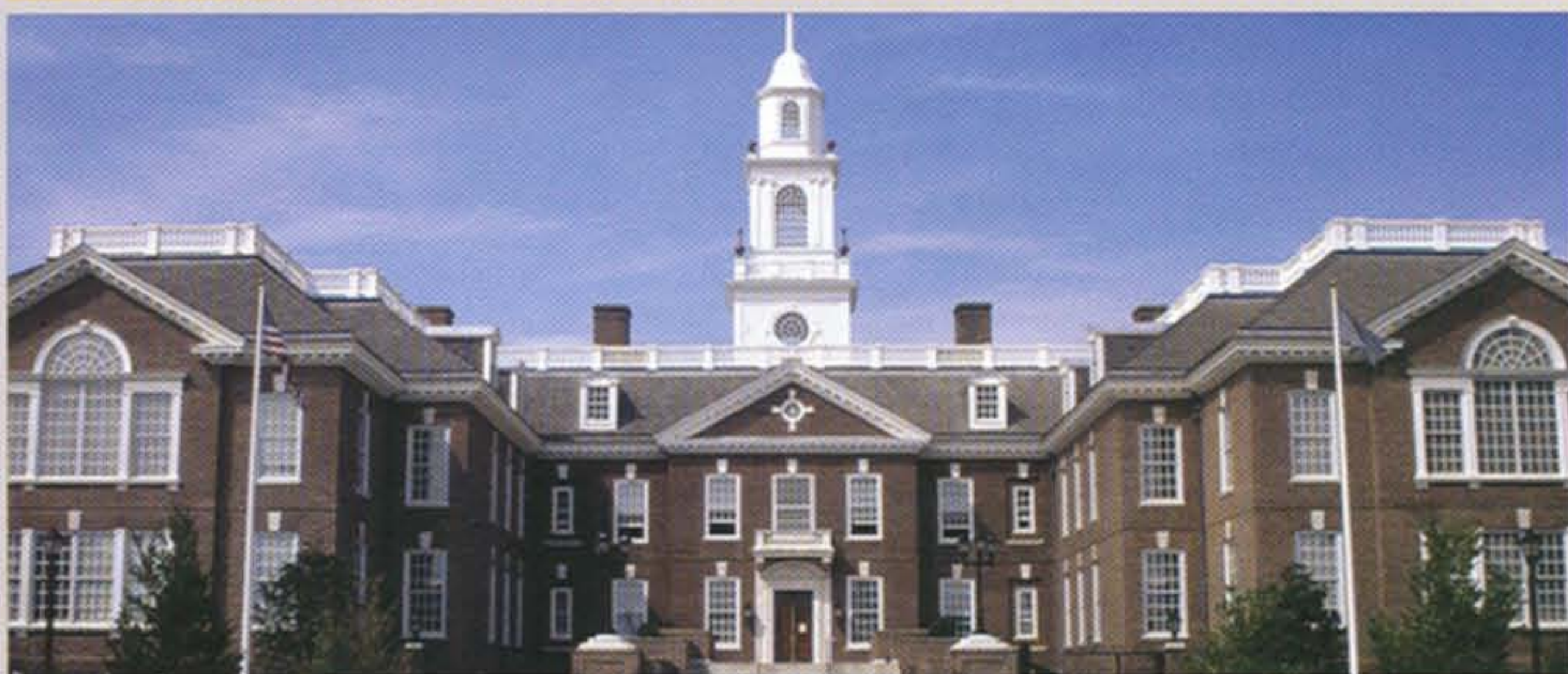


*Spotlight on:
Cyber Security for State Governments*



Spotlight

Delaware Department of Technology and Information (DTI) leads the way with a cyber security tabletop exercise

Ask some average citizens about “security” and, chances are, they’ll talk about protecting people and places from physical harm. But in today’s world, security is about more than just physical attacks. Now, security must also address sophisticated cyber threats that are harder to detect—but are equally dangerous.

Nameless, faceless cyber terrorists can strike from anywhere in the world. And, through their malicious, technology-based attacks, they can cause damage that matches or exceeds that of physical attacks.

For law-enforcement and other state and local government agencies, cyber threats have created a new set of challenges. Law enforcement agencies have clear policies and procedures for handling physical security.

But because cyber attacks involve complex technologies, detecting and responding to them is entirely different. Effective response requires a coordinated effort across numerous governmental disciplines.

How can state and local agencies adequately prepare themselves to prevent and respond to cyber security threats? As officials from Delaware’s Department of Technology and Information, (DTI) will tell you, *awareness* and *training* are key.

CTO Elayne Starkey and Disaster Recovery Coordinator Lisa Wragg recognized the importance of proactively addressing the new realm of cyber security. With that in mind, they planned and executed the State’s first Cyber Security Tabletop Exercise. Held in Dover in October 2005, the exercise involved 80 participants from approximately 10 agencies, two school districts, two universities and a private-sector financial institution. And, judging by post-event surveys, informal feedback and the State’s resulting focus on cyber security, the event was a resounding success.

To execute successfully, DTI worked in partnership with the Delaware State Police, the Federal Bureau of Investigation (FBI) and the Delaware Emergency Management Agency (DEMA), which provided an experienced moderator to facilitate the exercise. Another key partner was SunGard, which delivered consulting services throughout the planning stages, on-site support during the actual simulation and input into post-event reports and recommendations.

In this paper, Elayne and Lisa explain the approach and techniques they used before, during and after their cyber security exercise. They share some of the “lessons learned” as a result of the tabletop activities. And, they pass along some valuable tips for their peers who may embark on similar projects.

What is a Tabletop Exercise?

At its core, a tabletop exercise is a “dry run” to see how your employees and partners might respond to a situation, such as a cyber attack. Participants are grouped by functional area. Each group is provided a piece of the overall puzzle, and the teams must communicate and collaborate to determine the best course of action. Because the scenarios evolve throughout the day, an exercise can provide a fairly realistic assessment of how agencies would respond. It also provides a “safe place” to identify strengths and weaknesses.

Objectives

The goals of the State of Delaware Cyber Security Tabletop Exercise were to:

- Exercise the response and recovery capabilities of the State of Delaware and other supporting agencies/institutions surrounding a cyber attack
- Recommend/develop methods for all sectors (financial, law enforcement, government and education) to cooperatively protect the state’s critical infrastructures
- Determine and offer improvement to internal and external communication paths/plans
- Identify roles and responsibilities for all sectors

Before the Exercise

The idea for the tabletop exercise had been percolating since 2004, when Elayne and Dan Cox, former Deputy Secretary of the Homeland Security Department, repeatedly discussed the importance of cyber security. Then, in May 2005, DTI formally kicked off the project—giving the team five months to complete their plans and preparations.

According to Lisa, they used DEMA's established process, which includes an Initial Planning Conference (IPC), Midpoint Planning Conference (MPC) and Final Planning Conference (FPC). They also formed two planning teams: a core planning group that included Bob Moses from the Delaware State Police, Rob Underwood from DEMA, a variety of consultants from SunGard Availability Services and a DTI committee with representatives from the following groups:

- Applications Delivery (Programming Support)
- Business Office (Physical Security and Non-Digital Vital Records)
- Change Management (Communications)
- Customer Care Center (Customer Relationships)
- Data Center & Operations (System Support and Service Desk)
- Major Projects (ERP Systems)
- Systems Engineering (System Design)
- Telecommunications (Cyber Security and Network Support)
- Senior Team (Public Information Dissemination)

At the IPC, Lisa provided some education about tabletop exercises and solicited input about target objectives for the first one. Team members helped shape the objectives and identify potential scenarios to use during the exercise.

Before the MPC, Lisa fleshed out the scenarios so the core planning team could review them and make changes. She created five versions of the "playbook"—each reflecting a different functional area—as well as a Master Scenario booklet with a big-picture view. However, Lisa is quick to note that the DTI planning team members did not have an advance copy of the actual exercise prompts.

"The element of surprise is critical to a tabletop exercise," she explains. "If you reveal your scenario documentation beforehand, even the most well-intentioned person will read ahead and may prepare in advance. That can dilute the effectiveness of the exercise." Thus, the only folks who knew exactly what to expect were the handful of members on the core planning team.

Tips for Planning Success from the State of Delaware

- *Secure an executive sponsor before you begin planning your cyber security tabletop exercise.*
- *There are two ways to run a cyber security exercise: a broad, procedural approach or a drill-down, technical approach. For your first exercise, start with the broad approach.*
- *Hone in on your scenario early on—and stick to it. Seemingly "minor" changes have cascading effects on your playbooks, creating a lot of additional work.*
- *Expect to do some education about tabletop exercises. Assure invited participants and their managers that the exercise is well worth their time. Also, remind them that it will be a "safe" environment—not a time for finger-pointing or grandstanding.*
- *An expert third party, such as SunGard, can help provide fresh perspectives and insight when building scenarios for a tabletop exercise.*

During the Exercise

Following thorough planning and preparation, the DTI team and its partners were ready to execute on the full-day tabletop exercise. Individuals in the room were categorized in four ways—as participants, moderators, evaluators and observers—and were placed into logical groupings based on their roles and responsibilities. Moderators served as table leaders, guiding the discussion and serving as spokespeople to the larger group. Evaluators included subject matter experts from the agencies, as well as SunGard consultants, who shared their insight and observations during discussion. Observers included a variety of interested third parties, who were permitted to watch and listen—but not participate directly in the discussions.

Elayne kicked off the exercise by reminding participants that the exercise was intended to be a learning experience—not an opportunity for finger-pointing or “gotchas.” She then handed the platform over to DEMA’s Rob Underwood, an experienced facilitator of tabletop exercises.

In conjunction with Lisa, Rob guided the group through each of three, interrelated modules:

- Pre-event Preparation
- Event Detection and Response
- Event Recovery

Each module introduced key information and challenging discussion topics and questions about a variety of realistic cyber security threats. But with each group receiving different *pieces* of information, communication and collaboration among tables was critical.

According to Elayne and Lisa, there was a constant buzz of debate and activity in the room. Participants enthusiastically engaged in discussions, and as the modules progressed, interaction among tables reached a rapid pace. And the importance of communication became very apparent when one of the tables made a unilateral decision to shut down the network.

“Coming from a technical agency, I was very surprised by that decision,” Lisa says. “But it was quickly flagged as a problem and resolved. It was definitely an ‘a-ha’ moment that helped illustrate why cyber security is so complex.”

Elayne agrees, adding, “The issue about shutting down the network raised a key question: when it comes to cyber security, who’s in charge? Generally when there’s an emergency in the State, the law-enforcement agencies or fire departments lead the response. But with a cyber security incident—and all of the associated technical issues—DTI must lead the response.”

Another key moment occurred when participants proactively decided to implement a Command Center to address the evolving threats. A representative from each area was tapped to participate in this newly formed group. Lisa notes that she and her team had earmarked an empty table for a Command Center—and were thrilled when participants took the lead in creating one.

Indeed, both Elayne and Lisa were pleasantly surprised by the level of involvement of all participants.

“When people first came in, they were excited but also a little apprehensive. They thought they would be presented with something, have to come up with a response, and then be critiqued,” Lisa explains. “But once they realized no one was ‘critiquing’ them, they really opened up. They realized it was about awareness and communication.”

Elayne concurs: “Having that level of comfort was key to the success of the exercise. Everyone was candid and honest—and that led to much better results. Even the observers were highly engaged. They stayed close to the tables so they could hear the conversations in progress.”

DEMA’s Rob Underwood, who has led numerous physical security exercises, says he was overwhelmed by participants’ enthusiasm: “Most people had a good understanding of how important cyber security is. When a physical attack happens, it may affect one agency or organization. But with cyber security, it affects everyone—so everyone must be prepared to work together. This tabletop exercise was a great way to practice that kind of collaboration.”


During the Exercise

A “hot wash” session was held immediately after the exercise with involvement from DTI, Delaware State Police, DEMA, SunGard and the moderators from each table. With the information gathered there, two reports were drafted by DEMA—one with sensitive information and another “sanitized” version for wider distribution.

Ultimately, the State has realized several key benefits from the tabletop. First, Elayne and Lisa say that it set a solid baseline for future exercises. Going forward, they plan to execute a series of tabletop simulations.

Second, it led to some high-level “lessons learned”—namely, that there’s a need for:

- Additional training on cyber security.
- Formal policies and procedures.
- Better cross-agency communication and collaboration.



And, perhaps most importantly, due in large part to the tabletop exercise, cyber security is now top of mind in the State of Delaware. After the exercise, Elayne Starkey was asked to champion the effort of developing the framework for Delaware’s Information Security Program. Leveraging the results of the tabletop exercise—as well as her own in-depth research of other states’ efforts and best practices—she’s developing a statewide cyber security program.

Even within DTI, Lisa says the exercise has also helped increase business continuity and information security awareness: “Folks in certain disciplines don’t necessarily think about what I do every day as the DR coordinator. They’re usually focused on day-to-day, operational concerns. But, after the exercise, people gained a new appreciation for what we do and why it’s so important.”

Conclusion

Through thoughtful planning and execution, and working with a powerful team of partners, DTI has set a high standard for cyber security tabletop exercises. In a post-event survey of participants, the tabletop exercise garnered an overall rating of 4.56 on a scale of 1 to 5—underscoring the positive reactions to this event.

Working with other government agencies and SunGard, the Delaware team has demonstrated the power of these interactive sessions to illuminate strengths and weaknesses. And, they’re using the results of the exercise to help drive measurable positive impacts to cyber security.

Contributors

Gary Kenick
Regional Engagement Director

Frank Rothstein
Engagement Manager

Al Teufel
Strategic Account Executive

Steve Gill
Practice Manager, Information Security

Ron Schlecht
Lead Consultant, Information Security

Len Boyer
Lead Consultant, Business Availability

Bevan Cummin
Senior Consultant, Business Availability

Managing Editors

Pat McAnally
Senior Director, Product Marketing and
Thought Leadership

Catherine Trefz
Senior Marketing Manager, Product Marketing

SunGard Services

The SunGard Incident Management Exercise service provides a proactive means for your management and team members to test that personnel across agencies are aware, ready and equipped to perform the actions necessary to prevent or respond to a disruption to normal business operations. This service helps validate your readiness to effectively and efficiently manage incident response using your existing plans.

SunGard consultants work with senior management to identify your operational priorities and develop strategies to respond to specific challenges—which may include natural, technological, civil or environmental hazards.

Through meetings with senior management and agency/department representatives, SunGard tailors an Incident Management Exercise that addresses the following:

- Incident detection and preliminary assessment
- Notification and escalation
- Damage assessment
- Incident command center procedures
- Support activities
- Administrative procedures
- Resource requirements

In addition, SunGard reviews your existing incident response policies and procedures and recommends changes where appropriate. We also identify gaps between the capability needed to achieve response objectives and the exercise results.

About SunGard Availability Services

SunGard Availability Services is the pioneer and leading provider of Information Availability solutions helping to ensure uninterrupted access to mission-critical data and systems. We enable more than 10,000 clients worldwide to keep people and information connected through customized enterprise-wide solutions that support people, processes and infrastructure. We provide a complete portfolio of Information Availability solutions using over 3 million square feet of secure, redundant facilities supported by a 25,000 mile global network, 25 years of experience and over 2,000 expert resources in managed IT, professional and business continuity services. SunGard is known for helping customers get back in business quickly after an unplanned event. We're also the best qualified to help ensure that businesses never go down in the first place.

SunGard's Information Availability solutions help establish new standards to help keep systems, networks, applications and data always available and end-users always connected. SunGard can help customers achieve higher levels of availability, enterprise-wide solutions and lower total cost of ownership—all without giving up control or settling on one platform.

SunGard has led numerous simulations for clients in the private and public sectors. For more information on SunGard Availability Services and our Incident Command Services, please call 800-434-0002.

SunGard Availa

James Poffel, VP

505 Huntmar Park Drive, Suite 100
Herndon, VA 20170
Cell: (410) 882-3566
sas.governmentRFQ@sungard.com

Brian Blind, National Sales Mgr.

4500 Fuller Drive
Irving, TX 75038-6508
Office: (972) 650-8531
sas.governmentRFQ@sungard.com

SUNGARD®
Availability Services

©2006 SunGard Availability Services. All rights reserved.

The above material is presented as general information only and does not constitute legal advice or a legal opinion. You should seek the advice of legal counsel with respect to your particular circumstances.

ISL-002