

SUNGARD[®]
Availability Services

KEEPING PEOPLE AND INFORMATION CONNECTED.[®]

**Spotlight
on:**

**Cyber Security for
State Governments**

Delaware Department of
Technology and Information
Exercise Sharpens Skills for Cyber
Attack Prevention, Detection,
Response, and Recovery

Cyber attacks against public and private information technology and networks are escalating in occurrence and complexity every day. These threats manifest themselves in a variety of forms – including individuals operating as hackers and criminal organizations engaged in stealing data and identities, as well as national entities conducting cyber espionage and terrorists intent on bringing about harm to a government and its information systems.

Protecting against these threats is a multi-faceted challenge. Nameless, faceless cyber terrorists can strike from anywhere in the world without warning. And, those intent on doing harm never stop in creating new ways to attack systems, driving a constant need to improve skills, policies and tools that guide prevention, detection, response, and recovery.

In cyber security, overall security is only as strong as the weakest link, making it a requirement for coordinated planning and training across state and local government agencies. Yes, government organizations need firewalls, anti-virus software and other sophisticated technical tools. They also need strong security policies that monitor and report on attempted intrusions and other suspicious activities. It is critical to have a well-trained professional staff – across agencies – that can utilize the tools and policies – and work together in a synchronized way to address threats.

It is with this focus – sharpening the skills for prevention, detection, response, and recovery related to cyber attacks across state government agencies – that the Delaware Department of Technology and Information (DTI) conducted its fourth annual cyber security exercise in October 2008.

Delaware’s Chief Security Officer Elayne Starkey and Disaster Recovery Coordinator Lisa Wragg developed a tabletop and functional, hands-on exercise to address a set of escalating cyber security threats. Named “Web of Distrust,” the event brought together approximately 125 individuals from federal and state governments. In addition to state systems administrators, application personnel, telecom engineers and other personnel, the FBI, Army National Guard, members of the Delaware education community and SunGard

Availability Services participated. The event proved to be very successful in raising awareness of preparedness best practices among participants in addressing real-time cyber security threats.

On exercise planning and execution, DTI worked with the Delaware Emergency Management Agency (DEMA) and Delaware State Police. Another important contributor was the expertise of SunGard Availability Services, with SunGard providing consulting services during the planning process, on-site support as part of the exercise control team and observers during the event, and expert analysis in post-exercise reports and recommendations.

This white paper reviews the planning involved and the flow of events that took place during the cyber security exercise. It also outlines the lessons learned from the exercise – and provides valuable tips for other government agencies looking to conduct similar events.

Objectives

The goals of the State of Delaware cyber security exercise were to increase understanding and preparedness related to:

- Cyber incident detection, reporting and containment among the State of Delaware and other supporting agencies
- The incident command system utilized by state and local agencies during a cyber attack
- How to preserve electronic evidence to support computer forensic investigations
- Communications protocols to guide reporting, response and collaboration among agencies

What is Cyber Security?

Cyber security is defined as the protection of information against unauthorized disclosure, transfer, modification, or destruction – whether accidental or intentional. Some areas of great concern are data breaches, stolen information, and the inability to perform services during an extended outage.

Before the Exercise

In planning the exercise, DTI leveraged their experience from three previous cyber security events, but also wanted to take this event to a higher level by conducting both tabletop and functional exercises.

Elayne and Lisa kicked off the planning process six months before the exercise was scheduled to take place. DTI has a comprehensive exercise program, orchestrating events in disaster recovery from a physical outage, relocating critical departments to other facilities, and crisis communications as well as cyber security – so they are skilled in planning and execution.

According to Elayne, “Why do we test? The more we practice, the higher our skill level will be. It is not a question of whether the state will be hit by a cyber incident; rather it is a matter of when will we be impacted. We need to be prepared – and there is no substitute for practice to increase our readiness.”

They followed FEMA’s proven process for exercise planning which methodically maps out a Concepts and Objectives meeting (C&O), an Initial Planning Conference (IPC), Midpoint Planning Conference (MPC), and Final Planning Conference (FPC). DTI established a partner agency steering committee, which included the High Tech Crimes Unit of the State Police and DEMA.

At the C&O meeting, the concept and objectives of the exercise were developed – with the inclusion of a hands-on activity deemed to be critical to heightening the real-life simulation of a cyber threat. At the IPC, the concepts and objectives document was finalized and approved. Additionally, DEMA’s Emergency Operations Center was selected as the venue and potential exercise participants were reviewed.

“Our participants were a mix of IT professionals – to handle technical problems – and business managers – to address issues such as how to handle citizen calls regarding a cyber attack. This approach reinforces how essential it is for both groups to work together during a crisis,” said Lisa.

During the MPC, the master sequence event list was established and reviewed at an initial dry run – looking at the flow of activities during the exercise. Careful consideration was provided to how new scenarios would be injected into the exercise – to create a constantly changing environment where the threats

Closer Look at Cyber Security Exercise Components

The Delaware event included both tabletop and functional exercise components.

What is a Tabletop Exercise? A tabletop exercise is a “dry run” to see how 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 actions.

What is a Functional Exercise? A functional exercise provides an actual cyber attack on information systems and networks. It is conducted in a safe haven environment so there is no operational impact to actual IT infrastructure. The exercise provides hands-on training for learning how to detect and respond to threats in real time.

Tips for Planning Success from the State of Delaware

- Secure an executive sponsor before you begin planning your cyber security 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 that guide the exercise scenarios, creating a lot of additional work.
- Monitor security research and media coverage about the vulnerabilities you want to test. Exploits change often and you want to address current threats.
- Be sure to conduct dry runs and a dress rehearsal for a functional exercise – to identify glitches in time to be remedied.

escalated during the day. After the MPC, the detailed scripts of each inject were developed that the exercise control team would utilize during the event.

At the FPC, there was final review and approval of the full day’s scenario and logistics. A dress rehearsal was conducted allowing DTI to test the technical aspects of the computer injects that were to be used during the functional exercise. Also – with education being a top goal of the exercise – the presentations of expert sessions held during the day were reviewed to tailor them to complement the day’s series of activities.

During the Exercise

With comprehensive planning and preparation – as well as the experience from three prior tabletop cyber security exercises – in hand, the DTI team and its partners were ready to conduct the full-day exercise. Individuals at DEMA’s Emergency Operations Center were assigned to roles – participants, exercise control, moderators, evaluators, and observers. Participants included representatives from multiple state government organizations with a mix of IT and business personnel. None of the participants had any advance knowledge of the scenarios they would face during the exercise.

The exercise control team guided the day’s events initiating the multiple scenarios that unfolded during the day. Moderators floated throughout the exercise floor guiding participants if they needed assistance. Evaluators included subject matter experts from government agencies as well as SunGard Availability Services consultants who observed the day’s events and then shared their insights during the discussion period at the end of the day. Observers included a variety of interested third parties, who were permitted to watch and listen – but not participate directly in the exercise.

The exercise commenced with opening remarks from Elayne who shared the day’s goals:

- Sharpen skills to prevent cyber security attacks.
- Improve ability to rapidly detect, respond to, and recover from cyber security attacks.

Elayne stressed the exercise was a learning opportunity. DTI recognized participants had differing levels of readiness. The key measure was not how well each participant performed during the exercise, but rather how skilled everyone – individually and working as a

team – became after participating in the event.

Elayne discussed how this year’s exercise would include a functional exercise and she noted it would be a simulated IT system that provided a safe haven environment with no operational impact to any agency web sites. She also thanked Delaware Chief Information Officer and Secretary of DTI Tom Jarrett, noting how disaster training exercises need strong executive support to be successful.

Secretary Jarrett discussed with participants how IT’s world of risks is very different from physical hazards. And while Delaware is a coastal state that must always be prepared for natural disasters, data breaches and the potential harm they can do are also very real. Secretary Jarrett noted how vitally important it is to safeguard the agency and citizen data they are charged to protect which is why exercises like this event were so valuable.

Web site Defacement

The first thread of the exercise was kicked off with Lisa introducing a video news clip that was played to all participants on how there was a national alert related to a terror group from a simulated country with sleeper cells thought to be operating in the United States. The scenario unfolded with the Multi-State Information Sharing and Analysis Center (MS-ISAC) soon reporting Web site defacements across many state governments, with various states increasing their cyber alert levels.

After these events, Web site defacements began occurring across the simulated agency sites of exercise participants, displayed on the workstations in the operations center. The defacements altered the original home pages of agency Web sites. Defacements are typically the first visual indication that an application may have been tampered with by a non-authorized source. They also can be used to divert legitimate business to unauthorized sites for illegal purposes.

To make the situation dynamics even more turbulent, simulated citizen complaint telephone calls were flooded into all participating agencies about the Web site defacements.

Exercise control and observers noted the varying responses – such as one agency immediately hardened its server before the web infection took place and a school district placing a banner on its home page, saying the Web site was experiencing difficulties and providing a telephone number for people to call if they had questions.

DTI Public Information Officer Michele Ackles developed and issued a public statement that said state agency Web sites were experiencing defacements from outside interference. The statement urged all citizens to use extreme caution should they access government sites. DTI also said it was coordinating with law enforcement authorities to determine the attack source.

Immediately after the first thread of the exercise, an education session was held that reviewed the web defacement attack and provided an overview on cyber-vulnerabilities. Another training session focused on DTI’s Cyber Security Incident Response Team (CSIRT) process, which discussed incident handling and evidence preservation.

According to Elayne, holding education sessions immediately after an exercise activity is very important to the learning process. “We expect there will be different skill sets and levels among participants. These sessions provide a mechanism for people to learn the correct procedures while the event is still fresh in their minds. Plus, it gives them the opportunity to apply what was learned during the rest of the exercise,” said Elayne.

Data Breaches and Network Outage

Next, Lisa introduced the second thread as a tabletop exercise involving data breaches. This thread was triggered by a simulated MS-ISAC report that widespread hacking had occurred throughout many states utilizing Web-based Distributed Authoring and Versioning (WebDAV) on Web sites that have weak security credentials. The report also warned states were still experiencing this threat. The FBI soon followed with a simulated report that a terrorist group was attempting to discredit the United States by launching attacks against its IT infrastructure.

The participating agencies then began receiving citizen complaint telephone calls reporting identity theft after conducting business on Delaware state Web sites, and the news media called with inquiries to the Governor's office. This scenario drove participants to take steps in assessing how best to protect and secure systems from data breaches, and reviewing data retention plans that address corrupted or missing data.

During this thread, the exercise players established a Joint Information Committee to ensure a coordinated approach to develop and communicate a statement to citizens about the web site attacks, and steps the public should take to safeguard identities and report incidents to the police. This thread was followed by education sessions on how the Delaware State Police conducts computer forensic investigations and steps to take to minimize data loss incidents.

The third thread of the exercise was initiated with citizen complaint telephone calls saying they could not access government agency Web sites or the Web sites were unusually super-slow. Soon after, the day's cyber threats added a physical element with the state's entire computing network disabled by the terrorist actions of cutting service provider lines around the state. The situation's urgency was heightened because the event's timing threatened to disrupt national and state elections scheduled to take place in a few days.

State agencies depend upon networked computing resources in order to perform their day to day activities. This means network and server administrators need to be highly attuned to vulnerabilities, up to date on system patches, and have agreements with business counterparts on interim processes to be used in the event of an outage.

DTI took fast steps to relocate critical government customers to its facilities with operational computing environments so essential services could continue – without requiring the state-wide network. It also worked with the Delaware National Guard to tap the Guard's satellite network communications capabilities to provide networking services until its service providers were back online. Lastly, DTI coordinated with

the FBI, Delaware State Police and local law enforcement authorities to secure vital facilities and support the computer forensics investigation.

Reviewing Exercise Activities

Immediately after the exercise, a review session was conducted with participants from DTI, Delaware State Police, DEMA, and SunGard. They discussed both the exercise process and key points of learning how to address cyber security threats.

Looking at the process, there was widespread support for including a functional component to the exercise because it added a hands-on touch to the day's events. Additionally, it was viewed as important to include business and law enforcement participants in an IT exercise – so they could experience how technology disruptions can generate a significant impact on their jobs.

In addressing cyber security threats, communications protocols were identified as an area for improvement – particularly mapping communications paths between agencies to share information better and avoid operating in silos. As Elayne noted, "Having pre-established relationships before an incident happens is essential in emergency response. One big benefit from this cyber security exercise was it has started dialogues among the various government agencies and also with law enforcement authorities that need to work closely together in addressing cyber attacks."

Another key finding was how business continuity can play an important role in cyber attacks. According to Lisa, "As thread three unfolded, it became clear a critical question emerged: how did we plan to continue critical business functions without a state network? We need an 'all hazards' approach – be they fire, floods, cyber or anything else – to ensure business continuity."

Overall, the cyber security exercise exceeded the expectations of DTI and participating agencies. And it also reinforced the necessity for ongoing vigilance and training to stay prepared against the constantly changing array of cyber threats. As Elayne said, "We will definitely have a fifth annual cyber security exercise."

SunGard Services

The SunGard Incident Management Exercise service provides a proactive means for your management and team members to test that personnel across organizations 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

SunGard consultants are skilled in participating on exercise control teams to initiate and guide event scenarios. They also are experienced in serving as observers that monitor exercise events and provide clients with insights after the exercise on how to improve preparedness.

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

About SunGard Availability Services

SunGard Availability Services provides disaster recovery services, managed IT services, information availability consulting services and business continuity management software to more than 10,000 customers in North America and Europe. With four million square feet of datacenter and operations space, SunGard assists IT organizations across virtually all industry and government sectors prepare for and recover from emergencies by helping them minimize their computer downtime and optimize their uptime. We help organizations ensure their people and customers have uninterrupted access to the information systems they need in order to do business. To learn more, visit www.availability.sungard.com or call 1-800-468-7483.

SUNGARD® **Availability Services**

680 East Swedesford Road
Wayne, PA 19087
800-468-7483
www.availability.sungard.com