All Eyes: A Security Breach Exercise

Disaster Recovery/Security and Business Continuity Readiness

Commonwealth of Pennsylvania
Molly Dougherty, Director
Continuity of Government and Records Information Management
Pennsylvania Office of Administration
205 Finance Building
Harrisburg, PA 17120
modoughert@pa.gov
717.705.5590

Initiation: May 2014

Completion: June 2014

Executive Summary

Pennsylvania has lead and participated in numerous exercises to test and strengthen its cyber security posture. These exercises have generally focused on the IT response and remediation of an incident such as a data breach or distributed denial of service attack. However, the effects of a cyber-incident extend far beyond the IT department to include senior leadership, attorneys, program managers and others in the organization, as well as the public.

In 2014, Pennsylvania developed an exercise called “All Eyes” to specifically focus on the role of the chief information officer (CIO) in engaging and communicating with key stakeholders and decision makers during a cyber-event. The exercise was created jointly by Pennsylvania’s Continuity of Government Office and Enterprise Information Security Office and conducted with current and future chief information officers in the Certified Government CIO program at Harrisburg University of Science and Technology.

The exercise establishes a constructive environment for the students to learn about and prepare for the non-IT issues related to a data breach. Participants examine the responsibilities of the CIO, internal and external communications concerns, and the commonwealth’s security breach checklist of questions and potential actions to be taken during an incident.

The exercise package includes background information, checklist tool, exercise plan and presentation materials and is easily repeatable, allowing participants to further the discussion by hosting cyber continuity exercises of their own in their agencies.

Using Homeland Security Exercise and Evaluation Program (HSEEP) design principles, the exercise takes an “objectives-first” approach to exercise design ensure that the scenario, discussion and corrective actions achieve the following results:

- Understand the political and economic impact of a data breach and coordinated response.
- Review data breach reporting requirements.
- Examine command and control and communications challenges during a breach.

The no-cost exercise also followed the 70-20-10 model of learning development: (70% practice, 20% coaching/collaboration and 10% formal training)
.
The exercise encourages CIOs to view their role during a cyber-incident through a broader lens and familiarize themselves with the legal and communications aspects of a coordinated response. In doing so, the exercise strengthens both the commonwealth’s continuity and cyber response capabilities.

Through the inclusion of continuity planning and exercising in cyber strategies, Pennsylvania has been able to bridge the divide between IT disruptions and a coordinated response.

Business Problem & Solution

The frequency and severity of cyber incidents continues to rise, with 2014 dubbed by many as the “Year of the Data Breach.” With online services now the norm and demand for mobility and open data increasing steadily, Pennsylvania can only expect its exposure and risk to cyber threats to increase.

Recent history has demonstrated time and again that no one is immune to cyber threats. Like other governments, the Commonwealth of Pennsylvania has a responsibility and legal obligation to protect our employees and citizens and to continue essential business functions during natural, human-made or technological disasters.

Cyber incidents are a matter of when not if. Therefore, having a comprehensive, practiced response is critical. According to the 2014 Ponemon study, including continuity of operations in cyber security planning can help cut the cost of a data breach by up to $9 per compromised record.

Although the cyber incident itself may be an IT issue, the coordinated response extends far beyond the IT department. This is especially important for incidents involving the breach of data. Pennsylvania’s Breach of Personal Information Notification Act defines the conditions under which it is necessary to notify victims and credit reporting agencies. While an incident may be considered a ‘data breach’ from an IT perspective, it may or may not meet the definition of a data breach under the act.

In order to strengthen Pennsylvania’s cyber security readiness and ensure that IT leaders understand the fundamentals of a coordinated response approach, the Continuity of Government (CoG) office and Enterprise Information Security Office (EISO) partnered to design the “All Eyes” security breach exercise and conduct it with 26 students from Harrisburg University’s Certified Government CIO program, which includes current and aspiring CIOs from executive and legislative agencies and local governments. This easily repeatable exercise package includes background information, checklist tool, exercise plan and presentation materials.

Best Practice Exercise Design

The exercise scenario was tailored around the key learning objectives identified by the CoG office and EISO and developed using the nationally recognized Homeland Security Exercise and Evaluation Program (HSEEP) design doctrine:

- Understand the political and economic impact of a security breach and why a coordinated response is not merely an IT issue.
- Review security breach reporting requirements.
- Examine command and control and communications challenges during a security breach event.

The Scenario

The scenario was designed to be a realistic and probable so the discussion would focus on the response rather than the likelihood that such an incident could occur.

The exercise was structured as four modules and included discussions about who makes the legal determination of a data breach and the critical role of the CIO in communications.

Module 1: Lost but not Forgotten

The participants play the role of CIO of the organization. The exercise begins with notification of a potential security breach involving a little-known agency FTP site.

IT staff review the FTP site and identify a database that contains the names, Social Security numbers and home addresses of 5,000 applicants to a now-defunct energy assistance program.

Discussion questions focus on the role of the CIO during a potential data breach and how the commonwealth's Security Breach Checklist would be utilized at this stage of an incident.

Module 2: All is not Lost

Further review by IT staff finds that there has been some activity on the FTP site and that the applicants' data has been viewed. The CIO notifies the legal office that personal information may have been compromised.

Exercise participants are asked to assess the criteria for determining a security breach and what must be communicated – and to whom. Continuing to refer to the Security Breach Checklist, the group discussion explores the possible ramifications of a potential data breach, who makes the legal determination that a breach has occurred, who needs to be notified and why.

CIOs from multiple disciplines learned the answers to critical questions.

What is your role as a CIO during a potential security breach?

How would you use the security breach checklist at this point?

What are the possible ramifications if this is a security breach?

Who makes the legal determination that it is a breach?

At this point, who needs to know about the possible breach and why?

What is your communications plan if there is a breach in your agency?

Module 3: For all Eyes Only

Once the legal office has determined that the breach meets the definition under Pennsylvania's notification law, the discussion focuses on the communications plan and what information the chief information officer is responsible for providing.

Module 4: Lessons Learned and After Action

Based on lessons learned from the exercise, the participants were asked to develop action items for critical steps they must take in their agencies.

Through the inclusion of continuity planning and exercising in cyber strategies, Pennsylvania has been able to bridge the divide between IT disruptions and a coordinated response.

Significance of the Project

Effective completion of the cyber/continuity exercise and identification of corrective actions was a priority identified by Pennsylvania's Continuity of Government Steering Committee, which includes the Secretaries of Administration and General Services, Director of the Pennsylvania Emergency Management Agency; Commissioner of the Pennsylvania State Police and Commonwealth CIO. The All Eyes exercise focuses on resiliency by testing Pennsylvania's ability to communicate and establish a coordinated response during a potentially catastrophic event.

The exercise was designed using principles from the Homeland Security Exercise and Evaluation doctrine and included:

- **Training.** The exercise included a briefing on the cyber security threat landscape in Pennsylvania, the legal definition of a data breach and the impacts of declaring a breach.

- **Table Top Exercise.** Ground rules were designed to create an open, candid, low-risk environment that allowed participants to ask questions and discuss challenges.

- **Preparedness Tools.** Procedures and checklists have been created for CIOs to use when a breach occurs. Providing participants with an opportunity to practice using these resources while walking through the scenario is the most effective way to ensure familiarity aside from an actual event.

- **Continual Learning**. The after action review and development of corrective actions help to ensure implementation of lessons learned.

Benefits of the Project

In addition to supporting the CoG Steering Committee's 2014 program priorities, the exercise also aligns with the Pennsylvania IT Strategic Plan's emphasis on cyber security throughout its framework, as well as:

- NASCIO State CIO Priorities for 2014 – Security, including risk assessment and training and awareness, was the number one priority.

- The National Governors Association Call to Action for Governors for Cyber Security – Recommends taking steps to create a culture of risk awareness.

- National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity – Includes assessing risk, developing risk management strategy and providing awareness and training to personnel.

Pennsylvania has created an exercise tool and forum that can be easily replicated in other states that want to mature their security posture and further align operational readiness with priorities and FEMA exercise guidelines. All Eyes was developed around the following principles:

- **Effective and learning and development**. The no-cost exercise was designed based on effective learning research, including the 70-20-10 model of development. That is, 70% of the exercise encouraged practicing the response during a cyber-event, 20% on coaching and collaboration and 10% on formal training.

- **Successful practice.** Using the nationally recognized exercise design doctrine, Homeland Security Exercise and Evaluation Program (HSEEP), provided a consistent, tested method for effective exercise development.

- **Testing and practice.** Participants had an opportunity practice utilizing response procedures and tools in a "real world" but low-risk environment.