Portal Storm: A Cyber/Business Continuity Exercise

Cyber Security Initiatives

Commonwealth of Pennsylvania
Office of Administration
Tony Encinias, Chief Information Officer

Project Initiated: January 2013
Project Completed: December 2013
EXECUTIVE SUMMARY

Over the years, Pennsylvania has lead and participated in a number of cyber security exercises designed to test the organization’s response to remediating a cyber incident and communicating internally and externally about it. However, these exercises generally fall short in terms of capturing the business and continuity implications of a cyber incident, as well as engaging the highest levels of leadership.

Under the leadership of Governor Corbett, Pennsylvania is working aggressively to redesign its portal and expand the number of online services available to citizens and businesses. These new services are helping to reduces costs, increase efficiency and improve service. At the same time, they also increase the risk of service disruptions caused by technical problems or cyber incidents.

In an effort to mitigate these risks, the commonwealth’s Continuity of Government Steering Committee and the Office of Administration developed and led the implementation of a no-cost, comprehensive cyber-continuity exercise known as “Portal Storm.” The exercise was designed to increase awareness of risks and threats and ensure resumption essential government business, using alternate procedures if required.

The exercise was unique in that, rather than focusing on how the IT department responds to a cyber-attack, this exercise forced agencies to examine how their programmatic areas would continue to provide information and services during the attack.

Portal Storm included target training, table top exercises, executive briefings and after action reviews and corrective actions, all culminating with a briefing of all cabinet officials at the Governor’s residence.

Portal Storm has further elevated awareness of cyber security and business resumption across all levels of state government. Over fifty percent of all agencies identified roles and responsibilities that are unique to continuing essential services during a cyber event, and 80 percent of participating agencies were able to easily identify applications and business functions affected by the scenario and walk through and document alternate procedures. A significant number of agencies identified alternate procedures for their most essential services.

As a result of this comprehensive exercise, Pennsylvania is in a better state of readiness and posture for a cyber-event and has implemented corrective actions for the following capabilities: planning, impact assessment, and notification/communications. These improvements help to ensure that Pennsylvania state government is prepared to continue mission critical business services continue during a cyber-attack.
DESCRIPTION OF THE BUSINESS PROBLEM AND SOLUTION

The Commonwealth of Pennsylvania is a leader among states in the field of cyber security. However, we also recognize that we will never be completely invincible to attacks. Like other governments, we have a responsibility and legal obligation to continue essential business functions regardless of natural, human-made, or technological disasters. Pennsylvania is constantly evaluating and implementing protections from cyber-attacks. Attackers, at the same time, are constantly developing new and innovative ways to thwart these safeguards.

As state agencies continue to move government transactions and services online, we must increase our preparedness for a potential cyber-attack on our portal, with specific focus on understanding how an attack would affect agency functions and how agencies will continue to perform those functions while the portal is unavailable. **In essence, agencies must prepare to remain “resilient” during such an attack in order to ensure that essential government services and core business processes can continue to operate if and when an attack occurs.**

In 2013, there were over 30 disruptive events potentially affecting essential state government operations in Pennsylvania. Of those, 30 percent were cyber/network-related, including a brief denial of service attack on two agency websites. A coordinated response during a cyber-event requires involvement from agency leaders, information technology, communications, program staff and continuity planners, and the knowledge, training and skills required for each role are unique. Understanding the impact of a cyber-attack and the responsibilities for a coordinated response are business-critical activities and not strictly an IT issue.

Following the DOS attack, Pennsylvania's Continuity of Government (CoG) Steering Committee and the Office of Administration planned and conducted a cyber security/continuity of government exercise called “Portal Storm.” Portal Storm is a no-cost, comprehensive exercise designed to increase risk and threat awareness and ensure resumption of essential government business, using alternate procedures if required.

At its core, the Portal Storm exercise is about resiliency – testing Pennsylvania's ability to cope with the loss of the ability to deliver information and transact services through its websites and gaining a better understanding of how business and communications would continue to function. By tying real-world cyber security threats to potential adverse and severe impacts to the business, Portal Storm raised awareness across all levels of state government, elevated cyber security to a Governor and cabinet-level issue and enhanced our overall preparedness for a potentially crippling cyber-attack.

Effective business resumption requires awareness of threats and risks, as well as the ability to fulfill the required roles and responsibilities. Because the skillsets required by agency leaders, information technology, communications, program staff, and continuity
planners differ greatly, we recognized that a “one size fits all” approach to training was not possible.

Additionally, the benefits of an exercise performed as a single “activity” with a fictional scenario has only short term results. As a result, the CoG Steering Committee insisted that Portal Storm include targeted training through practice and the incorporation of corrective actions into future testing, training and exercise plans.

Portal Storm was designed using principles from the Homeland Security Exercise and Evaluation doctrine and included:

- **Training.** Leveraged online conference technology to implement targeted awareness training and exercise briefings.
- **Table Top Exercises.** Held discussions with multiple levels of government including members of Governor Corbett’s senior staff and cabinet, agency deputy secretaries, chief information officers, chief information security officers and agency continuity managers, on how they would respond to a cyber-attack that would greatly reduce or deny the delivery of online transactions or services.
- **Agency executive preparedness.** Agencies provided readiness briefings to their executive leadership.
- **Continual learning.** Utilized after action reviews and corrective actions development to ensure implementation of lessons learned.
- **State executive training and practice.** The exercise concluded with a briefing during the Governor’s cabinet meeting at the Governor’s residence.

The exercise incorporated a real world scenario and was conducted in a real world environment. That is, rather than selecting a few participants from each agency and hosting an exercise in an isolated conference room, IT employees, continuity planners and program staff in state agencies received targeted briefings and trainings based on their roles.

Agencies were instructed to work through the scenario and answer questions over the course of six weeks and brief their cabinet head on the continuity capabilities and corrective actions. Questions related to the scenario included:

1. Impact to operations
2. Command and control
3. Notification/communications
4. Documented alternate procedures
5. The inclusion of cyber-attacks in the agency continuity plan

The intent of the exercise was to make sure agencies understand their risks and identify ways to continue to carry out business operations during an attack. As a result of the exercise, over half of the participating agencies have included follow up cyber-continuity exercises and disaster recovery tests in the testing, training and exercise plans submitted with their annual agency continuity plan updates.
SIGNIFICANCE TO THE IMPROVEMENTS OF THE OPERATION OF GOVERNMENT

By integrating impact to essential government business into the exercise, Portal Storm provided a forum for state leaders to determine where immediate investments must be made in regards to cyber-security and our readiness posture.

Effective completion of the cyber/continuity exercise and identification of corrective actions was a key part of the CoG Steering Committee’s 2013 program priorities. The exercise also aligns with Pennsylvania’s IT Strategic Plan, which emphasizes security throughout its strategic 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 creating a culture of risk awareness.

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

By using the Homeland Security Exercise doctrine, Pennsylvania has created a tool and forum that can be easily replicated in other states that need to mature their security posture and further align operational readiness with priorities and FEMA exercise guidelines. Portal Storm was developed around the following principles:

- **Effective and learning and development.** The no-cost exercise was designed based on effective learning research. The Cyber storm exercise was based on 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.

- **Horizontal and vertical coordination.** The exercise encouraged employees at all levels to practice and learn in a no-fault environment. The exercise engaged multiple disciplines and levels of positions in all cabinet agencies including: information technology staff, continuity managers, program/business owners, agency CIOs, and senior level agency heads, including the Governor’s cabinet.

- **Successful practice.** Using the Homeland Security Exercise and Evaluation Program (HSEEP) doctrine provided the ability to test assumptions and implement corrective actions learned from the exercise.

- **Improved understanding of risk and impact.** Leveraging our enterprise unified communications system, trainings were held in a webinar format, allowing further reach with minimal cost.
• **Resilience.** Assuming not “if” but “when”, the exercise included an evaluation of documented alternate resources for cyber-dependent functions.

**BENEFIT OF THE PROJECT**

As the focus for the exercise was on preparedness for when an event happens, the benefits reflect the commonwealth’s resiliency and preparedness rather than preventing an attack. As a result of the comprehensive exercise:

1. The CoG Steering Committee was able to determine the readiness posture for a cyber-event and perform corrective actions in the following areas: Planning, Impact Assessment, and Notification/Communications.
2. Over half of the agencies identified key roles and responsibilities for a cyber event in their continuity plan.
3. Eighty percent of agencies participating were able to easily identify applications and business functions affected by the scenario and document alternate procedures if necessary.
4. Command, control and communications were identified as primary capabilities requiring improvement. Many agencies will be confirming the role for the incident commander and developing communications plans for an event.
5. A number of agencies are building on what they learned during Portal Storm. For example, one agency found the scenario did not affect many of its essential services and was able to leverage that knowledge to engage agency executives in discussions regarding investment in other critical systems.

Most importantly, the exercise helped and continues to help Pennsylvania assure its citizens that the services they rely on, such as unemployment compensation, public safety operations, and healthcare, will continue through alternate procedures and contingencies, which can only be determined through an exercise such as Portal Storm.

<table>
<thead>
<tr>
<th>Portal Storm Activities</th>
<th>Outreach and Participation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resilient Accord cyber preparedness workshop</td>
<td>65 IT and continuity employees from 30 different agencies participated in this workshop.</td>
</tr>
<tr>
<td>Online training</td>
<td>Over 250 IT, program, and continuity employees from 30 different agencies participated in the online training.</td>
</tr>
<tr>
<td>Scenario review, identification of impact to operations, and alternate procedures</td>
<td>CIOs, continuity managers, and program staff from 25 different agencies participated.</td>
</tr>
<tr>
<td>25 agency-led executive briefings</td>
<td>Individual briefings were held with each agency including the cabinet head, chief information officer, deputy secretary for administration and continuity manager.</td>
</tr>
<tr>
<td>Cabinet briefing and exercise</td>
<td>The Governor and cabinet heads from 25 agencies and the Governor’s senior staff participated.</td>
</tr>
</tbody>
</table>
After action review and corrective action development

25 agencies have developed and documented corrective actions included in the testing, training and exercise plans for 2014.

In conclusion, Pennsylvania has always had a robust and mature cyber security program to secure its IT infrastructure, but even the best and most prepared programs can fail if all of the participants are not aware of the program’s capabilities and weaknesses. This is why it was essential for us to host exercises that involve cabinet-level staff and agency deputy secretaries.

These individuals are the decision makers for our organizations and it was essential that they be part of the Portal Storm exercise so they could understand the threats posed by cyber-attacks and participate in the mitigation processes that came from the table-top exercises. This exercise has had the following benefits:

- Cabinet level advisors and executive level managers were provided cyber security awareness training via the exercise.
- The importance of IT transactions and services were clearly identified and discussed, resulting in a Business Impact Analysis (BIA) on what would happen if IT services were disrupted or out of service for a significant amount of time.
- The BIA helped the CoG Steering Committee and CoG planners re-evaluate their plans and take into consideration how potential interruptions in IT services could impact governmental operations.
- Agency CoG Planners and IT personnel worked collaboratively to create communication/mitigation strategies to address how they would continue to operate effectively until IT operations could be restored.
- Pennsylvania has become much more resilient and better prepared for a cyber-event impacting government business operations.
- A heightened awareness of cyber-security beyond the IT community.
- The lessons learned have become an integral part of the Pennsylvania’s IT Strategic Plan, as well as the National Governor’s Association’s Cyber Security Call to Action, NIST Cyber Security Framework, and NASCIO priorities for states.

Pennsylvania believes the exercise could be emulated by other states and welcomes the opportunity to share its approach and lessons learned or to help establish similar exercises.

Through Portal Storm, we have learned we are only as secure the rest of our cyber-community and we believe our experiences can help other government entities align cyber security to vital business functions and strengthen their cyber postures, which in turn bolsters our national cyber readiness across the country.