2015 NASCIO AWARDS

Title: Cyber Assessment and Measuring Success
Cyber-Disaster Recovery Continuity of Operations Assessment Tool

Category: Disaster Recovery/Security and Business Continuity Readiness

Contact: New Jersey Office of Information Technology
Office of the Chief Information Officer
E. Steven Emanuel, CTO/State CIO
609-777-5865
Steve.Emanuel@oit.nj.gov

Additional: John A. Essner, New Jersey Office of Information Technology
Chief Information Security Officer
609-633-9210
John.Essner@oit.nj.gov

Initiation: September 2014

Completion: December 2014

EXECUTIVE SUMMARY

NEW JERSEY CREATES CYBER-DR-COOP ASSESSMENT TOOL: SHARES IT WITH OTHER STATES

New Jersey has created a new Cyber-Disaster Recovery-Continuity of Operations (Cyber-DR-COOP) Assessment survey tool that it is sharing with other States. The survey is a self-assessment questionnaire designed to identify strengths and weaknesses in agency preparedness in Cyber Security, IT Disaster Recovery, and IT Continuity of Operations, and provides data for comparisons of best practices. When the survey was first developed, no other assessment model existed with this type of methodology.

In September 2014, the New Jersey Office of Information Technology (OIT), in partnership with the New Jersey Office of Homeland Security and Preparedness (OHSP), began its second annual (Cyber-DR-COOP) survey. New Jersey shared the model with California, Delaware, Pennsylvania and the Multi-State Information Sharing Analysis Center. In the summer of 2015, NASCIO plans to feature the model in a Security Conference call with both private- and public-sector participants.

The 2014 assessment results, improved government security operations as survey managers prioritized and incorporated their findings into the State of New Jersey Executive Branch's Security Framework. The risk assessment offers at-risk agencies mitigation strategies based on the Framework's categories and subcategories.

OIT is committed to emergency preparedness and will continue its self-assessment and planning on an annual basis. OIT's mission is to enable all the agencies of New Jersey State government to deliver services reliably and efficiently by providing them with cost-effective administration of Information Technology services within the Executive Branch.

BUSINESS PROBLEM AND SOLUTION DESCRIPTION

New Jersey's effort began shortly before Super Storm Sandy battered the state in October 2012. OIT and OHSP began to evaluate the State's cyber security and emergency preparedness in Information Technology across the Enterprise. Sandy provided an unprecedented, real-world test of how well the State's IT infrastructure, personnel and procedures would perform during a significant natural disaster. Sandy's landfall reinforced the critical need for an accurate and complete assessment of State IT preparedness.

After the storm, OHSP and OIT resumed the development and data gathering process with the goal of creating an assessment tool for measuring State's readiness in the three primary areas of Cyber Security, IT Disaster Recovery and IT Continuity of Operations.

OIT and OHSP developed the questionnaire by using Gartner's Leadership Maturity Model, a time-tested system that utilizes rational metrics. The model has eight subcategories including Essential Functions; Implementation, Leadership and Delegation, Facilities, Communications, Vital Records, Training and Exercises, and Program Management. OHSP and OIT distributed the criteria for each of the three key assessment areas, describing the questions included within each of the eight subcategories. Each assessment question retained four possible responses based on the colored maturity level.

	GREEN (Proactive and Sustained)
	YELLOW (In Progress/Maturing)
	ORANGE (Improvements Required)
	RED (Significant Risk)

In 2013, the first (Cyber-DR-COOP) assessment survey tool was completed by the agencies and departments, and New Jersey used the results to create a baseline for future surveys. Additionally, OIT and OSHP used the results to come up with a list of the Top 10 risks for Cyber Security.

In September 2014, OIT and OHSP launched its second-annual Cyber-DR-COOP survey. The agencies and departments submitted their answers, and the scores were totaled and charted in the three key assessment areas, the eight subcategories and the four maturity levels. The results were presented to the State of New Jersey's Treasurer, the Executive Branch Chief Information Officer Collaboration Council, and the Cyber Security Threat and Mitigation Committee.

SIGNIFICANCE TO THE IMPROVEMENTS OF THE OPERATION OF GOVERNMENT

SURVEY INCORPORATED INTO SECURITY FRAMEWORK

Using the 2014 assessment results, the survey managers prioritized and incorporated their findings into the State of New Jersey Executive Branch's Security Framework. The risk assessment offers at-risk agencies mitigation strategies based on the Framework's categories and subcategories. The Security Framework follows and establishes security standards and best practices based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework. It should be noted that the State of New Jersey's Executive Branch also has established a Cyber Security Strategy Plan (CSSP).

Risk Priority ID	Security Framework Subcategory	Risk Detail Description	Likelihood (H,M,L)	Business Impact (H,M,L)	Mitigation (Analysis/Recommendation)	Resources	Completion Time	Mitigation Acceptance	Status	Tier 1: Partial	Tier 2: Risk Informed	Tier 3: Repeatable	Tier 4: Adaptive
1													
2													

Function	Category	Subcategory	State of New Jersey's Security Controls	Current Profile	Risk Priority ID	Target Profile
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected				
		PR.DS-2: Data-in-transit is protected				
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition				

BENEFITS OF THE PROJECT: READINESS IS KEY TO FUTURE SUCCESS

Technology advances, government priorities shift, and new challenges constantly emerge. Among Sandy's lessons is that OIT must continue to plan for challenging situations even when a crisis hits and seeing beyond immediate needs is near impossible. Clearly, once such an event is past, OIT must instantly begin to ready the State's IT infrastructure and systems for the inevitable challenges and emerging opportunities that will follow.

The Cyber-DR-COOP assessment survey and results, and the Cyber Security Strategy Plan and Security Framework will assist OHSP and OIT in making improvements in cyber security and ensuring those efforts and controls are factored into New Jersey's cyber security, disaster recovery, and continuity of operations readiness.