NASCIO 2015 State IT Recognition Awards

2015 Award Nomination

Title: **Idaho Transportation Department Cyber Security Program**

Category: **Cyber Security**

Contact: **Shannon Barnes, CIO**
Idaho Transportation Department
(208) 334-8771
shannon.barnes@itd.idaho.gov

State: **Idaho**

Initiation Date: **January 5, 2014**

Completion Date: **November 1, 2014**

— ITD Cyber Security Program —

Executive Summary

The goal of the Idaho Transportation Department's (ITD) Enterprise Technology Services (ETS) is: *"To continuously improve the security and accessibility of the technology infrastructure and information they store and manage, both for Idaho citizens and the department's mission-critical public-safety partners."*

To reach this goal, ETS utilizes the National Institute of Standards and Technology (NIST) Cyber Security Framework to define the standards, policies, processes, and tools needed to create an effective Cyber Security Program for ITD.

The Cyber Security Team established ITD-specific security requirements based on the business needs of the department. They completed specific compliance criteria, established performance metrics and goals for each NIST function, and conducted a department-wide assessment to establish ITD's baseline compliance. The Cyber Security Team then adjusted their work activities to focus on areas where the most work was needed to meet the goal.

The team conducts quarterly assessments and updates performance metrics to track progress towards achieving ITD's security goals. The performance metrics and goals are posted in highly visible locations creating conversations across all ETS teams regarding the successes and challenges of keeping ITD secure from cyber security threats.

ITD executives also review the security metrics in an effort to understand and make educated decisions on the financial and human resources needed to support the program.

ITD has been recognized by the Transportation Research Board, a division of the National Academies of Sciences and Federal Highways Administration, as the first state agency in the nation to implement the NIST framework in such an effective manner.

The department's Cyber Security Team has provided national webinars on the subject, and has been asked to speak at several national conferences outlining their implementation of the NIST framework.

ITD’s Cyber Security Program

BUSINESS PROBLEM AND SOLUTION

Problem

The Idaho Transportation Department’s Executive Team issued a direct question to the Cyber Security Team:

“How can we demonstrate return on investment for the dollars and human resources being invested in the Cyber Security Program?”

To answer the question, the team realized they would need to utilize an industry standard framework and develop a way to measure and track the department’s performance towards achieving its cyber security goals in the most cost effective manner.

Solution

The department’s Cyber Security Team began their journey to understand what was needed to set up an effective Cyber Security Program by requesting assistance from ITD’s Internal Audit Team. They did this to ensure an objective and independent point of view.

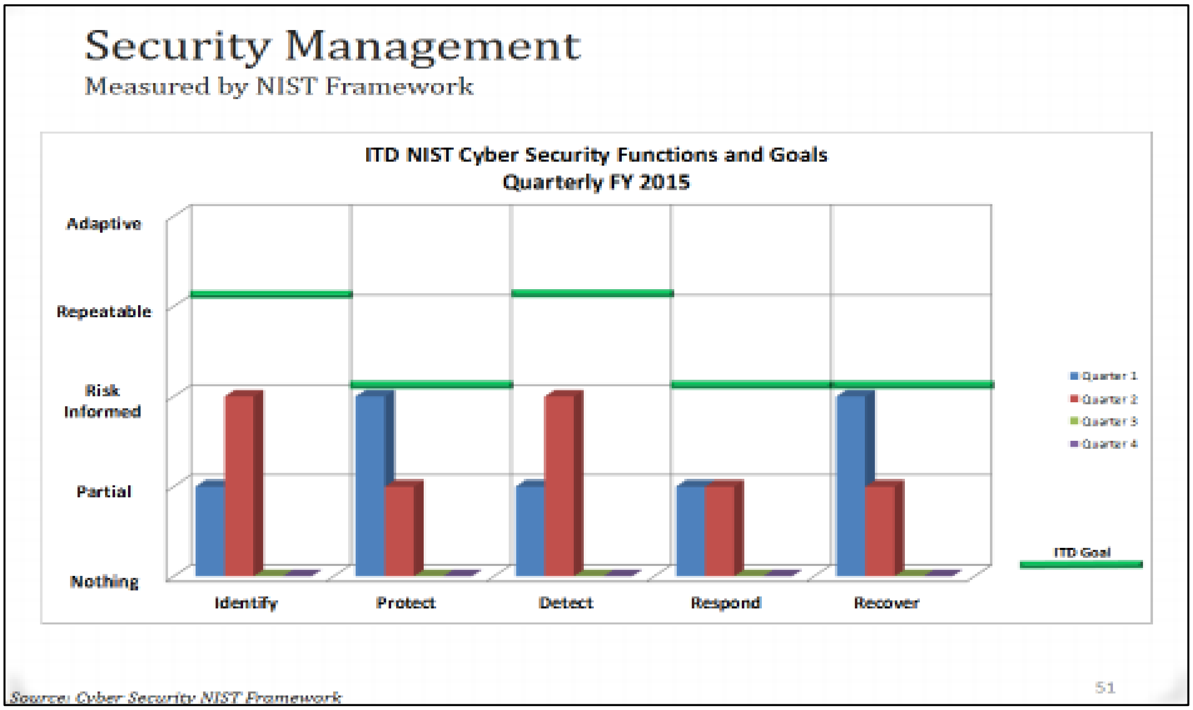
The team reviewed and analyzed several different types of frameworks, but decided on the *NIST Framework for Improving Critical Infrastructure* as it was adopted by the federal government and the State of Idaho. Once that decision was made, the team researched state and federal laws and interviewed subject-matter experts in each business area to define ITD’s security requirements and determine the level of compliance needed in each of the following NIST functions:

- **Identify**
- **Protect**
- **Detect**
- **Respond**
- **Recover**

The first step was to establish ITD’s baseline compliance according to the previously established security requirements and compliance criteria in each NIST function. Goals and metrics were then established to track and measure the team’s progress. Visual-management charts were created to show ITD’s strengths and weaknesses in each function and where work activities need to be focused.

The team conducts quarterly assessments and updates the performance metrics that track progress towards achieving ITD’s security goals. The performance metrics are posted in highly visible locations for all to see and better understand the progress—and the amount of work remaining to achieve the goals.

The graph below shows each of the five NIST functions, ITD's rating in each function, the goals, and the progress towards each goal on a quarterly basis.



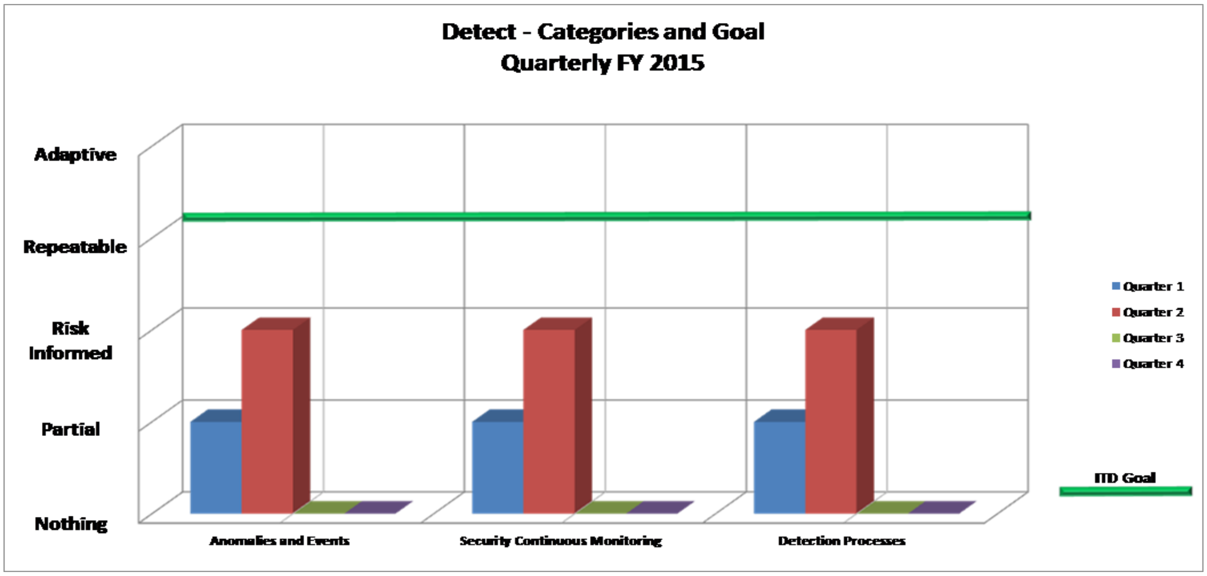
Security Management

Measured by NIST Framework

Source: Cyber Security NIST Framework

51

The graph below shows an example of the "Detect" function that is the next level of detail in the NIST framework. The graph's data originates from highly detailed Excel spreadsheets containing the security requirements, the compliance criteria, and a complex mathematical calculation that determines the current level of compliance.



SIGNIFICANCE

The significance of ITD’s Cyber Security program is its ability to clearly communicate to executives the value cyber security provides in identify and mitigating security risks that are directly related to safeguarding Idaho’s highway system and protecting citizen information. The program contributes to their understanding of the necessity of implementing security policies and procedures that can be perceived as restrictive and burdensome and clearly demonstrates the return on investment.

The program is credible because the team has created a simple way to show executives how ITD’s security status compares with a national, industry-accepted framework.

Cyber security has become a critical component in managing the nation’s transportation system as more and more of the system relies on Intelligent Transportation Systems (ITS) such as traffic signals, cameras, and dynamic messaging signs to manage the highway system.

ITD is also responsible for securing personally identifiable information (PII) for motor vehicle owners and drivers. The NIST framework, security requirements, metrics, and goals have given ITD a clear understanding of the work and financial support needed to protect its assets.

The program the team developed is serving as a model for other state agencies.
The Idaho Transportation Department has been recognized by the Transportation Research Board, a division of the National Academies of Sciences and Federal Highways Administration, as the first state agency in the nation to implement the NIST framework in such an effective manner.

The department’s Cyber Security team has provided national webinars on the subject, and has been asked to speak at several national conferences outlining the implementation of the NIST framework, and how it can help other transportation agencies protect their technology infrastructure.

BENEFITS

Cyber security programs are expensive and need more and more human resources to manage the program. The visual management graphs show executives the return on investment provided by cyber security. This allows them to see that they are not just throwing money into a black hole and hoping for the best, because they can see quantifiable improvement for the money spent.

When ITD’s baseline compliance was first established it showed that cyber-security resources were being focused on areas in which the department was already performing well, instead of the areas that needed the most improvement. As a result, human and financial resources were shifted to areas that needed improvement.

The NIST framework, security goals, and performance measures provide ITD with an excellent management tool that helps management decide where best to allocate resources to achieve the maximum return on investment.

All levels of the organization now understand the resources required for ITD to identify security risks, implement appropriate safeguards, and recover from a cyber-security event.

ITD executives are able to make educated and risk-based decisions when determining the level of financial and human resources needed. There is no framework and no amount of goal-setting that will protect ITD from all cyber security threats, but for the first time, ITD has a clear understanding of its current risk profile and what must be done to improve it.