Using the NIST Framework for Metrics

5/14/2015

ITD - Public Safety

- Safety improvements reduced total crashes by 29% and injury crashes by 41% in corridors after GARVEE projects were completed
- Ads / Commercials

ITD - Winter Driving

- Idaho's largest snow removal service: 12,284 lane miles

- Roads covered:
  - Interstates (like I -84)
  - US Highways (like US 95)
  - State Highways (like SH 21)
- Includes 1824 bridges.

2014 Orange Barrel Migration Season

- $284.5 Million dollars of construction projects
- 430 lane miles
- 39 bridges rehabilitated

DMV

- 1.11 Million licensed drivers
- 1.63 Million registered vehicles

Aeronautics

- 2400 (approx.) registered aircraft
- 5900 (approx.) registered pilots
- 126 public use airports
- 31 State operated airstrips

One last statistic

- 15.8 Billion vehicle miles traveled in on Idaho's freeways in 2014

What is a Cybersecurity Framework

- A collection of existing standards, guidelines and practices for reducing cyber risks to critical infrastructure.

Why use a Cybersecurity Framework

- A lot of money was spent on gathering really smart people to document what worked and what did not work to protect their technology infrastructure

What is the NIST

- National Institute of Standards (nist.gov)
- Non-regulatory agency of the US Department of Commerce
- Mission: Promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

What is the NIST Framework

- NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.0
- Released February 12th 2014

- The national and economic security of the United States depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. Similar to financial and reputational risk, cybersecurity risk affects a company's bottom line. It can drive up costs and impact revenue. It can harm an organization's ability to innovate and to gain and maintain customers.

- To better address these risks, the President issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," on February 12, 2013, which established that "[i]t is the Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties." In enacting this policy, the Executive Order calls for the development of a voluntary risk-based Cybersecurity Framework – a set of industry standards and best practices to help organizations manage cybersecurity risks. The resulting Framework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses.

What we were doing before NIST

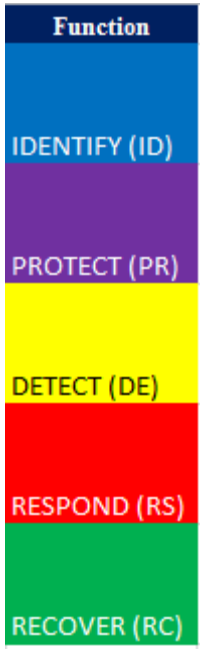
- We were using the ISO/IEC 17799:2005 and ISO/IEC 27001:2005
- Other Idaho State Agencies using the SANS top 20 Critical Security Controls
- ITD IT Auditors using CoBIT

Why use NIST

- Federal Agencies (Including FHWA) use the NIST Framework
- NASCIO supports adoption of the NIST Framework
- Other Idaho State Agencies were considering using the NIST Framework
- Needed to update ISO Framework (not free)
- NIST Framework (free)

NIST Framework Details

- Functions



"**Functions** organize basic cybersecurity activities at their highest level. These Functions are **Identify**, **Protect**, **Detect**, **Respond**, and **Recover**. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities. The Functions also align with existing methodologies for incident management and help show the impact of investments in cybersecurity."

NIST Framework Details

- Functions
  - Categories - **"Categories** are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities."

RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

NIST Framework Details

- Functions
  - Categories
    - Subcategories –"**Subcategories** further divide a Category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each Category."

RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after an event
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned
		RC.IM-2: Recovery strategies are updated
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Public relations are managed
		RC.CO-2: Reputation after an event is repaired
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams

NIST Framework Details

- Functions
  - Categories
    - Subcategories
      - Controls – "**Informative References** are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory. The Informative References presented in the Framework Core are illustrative and not exhaustive. They are based upon cross-sector guidance most frequently referenced during the Framework development process."

RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after an event	COBIT 5 DSS02.05, DSS03.04 NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	COBIT 5 BAI05.07 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RC.IM-2: Recovery strategies are updated	COBIT 5 BAI07.08 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Public relations are managed	COBIT 5 EDM03.02
		RC.CO-2: Reputation after an event is repaired	COBIT 5 MEA03.02
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	NIST SP 800-53 Rev. 4 CP-2, IR-4

NIST Framework Details

- Functions
  - Categories
    - Subcategories
      - Controls

- Rated by Tiers

Tier Score	Tier
0	Nothing
1	Partial
2	Risk Informed (Communicated)
3	Repeatable
4	Adaptive

What is a metric?

- “Performance metrics measure an organization's activities and performance. It should support a range of stakeholder needs from customers, shareholders to employees.” - Mark Graham Brown, *Using the Right Metrics to Drive World-class Performance*

Why does a Cybersecurity program care about Metrics?

- Shows us how we are doing
- Allows us to set goals
- Shows us how we are doing over time
- Security programs are expensive and metrics show executives they are not just throwing money into a black hole and hoping for the best

Why use the NIST Framework to make metrics?

- Our existing metrics were not very useful, we needed to show how the previous cybersecurity metrics affected day to day operations

How we metricized the NIST Framework

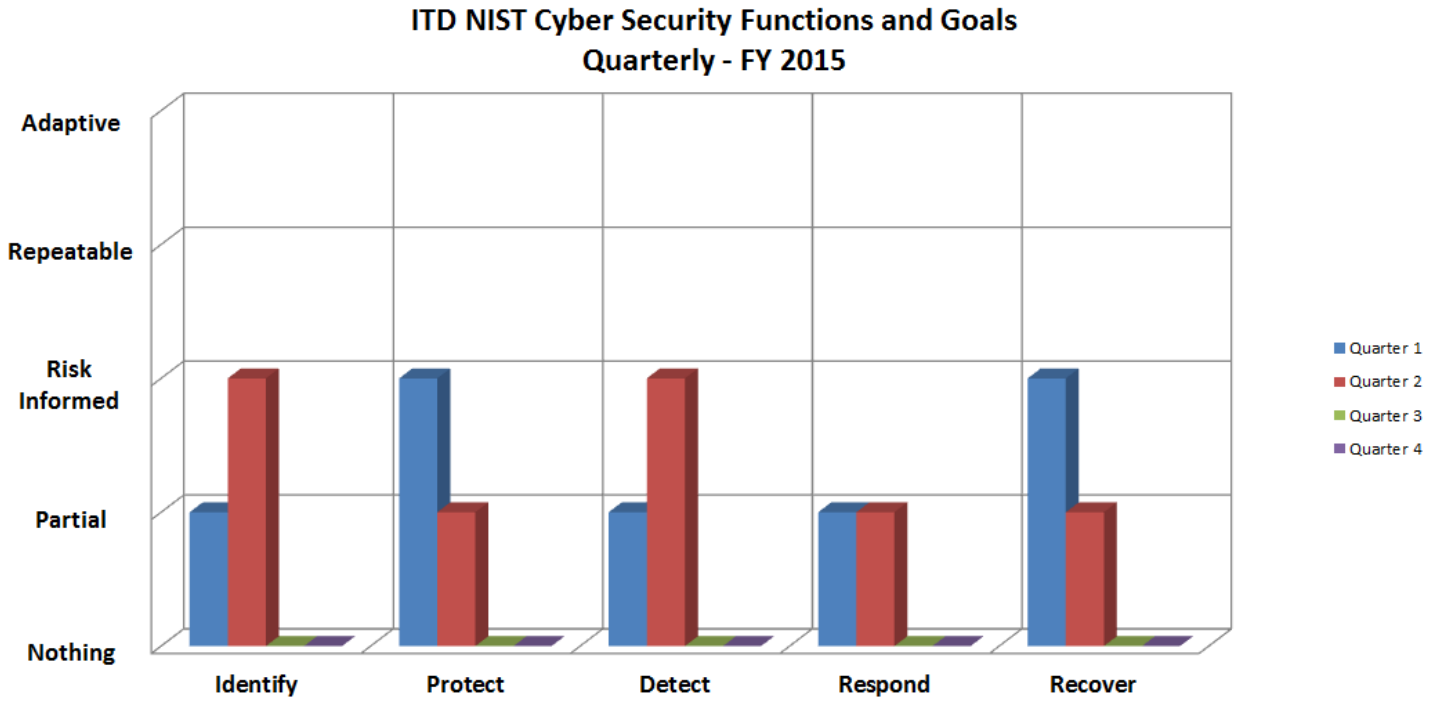
- Planning
  - We developed a matrix (Excel spreadsheet) to help us evaluate the framework by Sub Category by Tier
  - We Baselined (took a really quick guess) at where we were on the framework
  - We set (aggressive) goals on where we would think we should be in 3 to 5 years
    - Set goals by Function
      - Drove Goals down by Category

How we metricized the NIST Framework

- Scoring
  - We created a method of scoring the NIST by numeric value of the Tier (0 through 4) by Sub Category.
    - We score Categories by taking the floor (rounding down) of the average of the component Sub Categories. This gives us a conservative view on the Category.
    - We score Functions by taking the floor (rounding down) of the average of all the component Sub Categories. This gives us a conservative view of the Function. We don't average the Category scores because averaging averages is mathematically bad and causes a dilution of precision that would make anybody look really bad. (Our goal was to be conservative not pessimistic.)

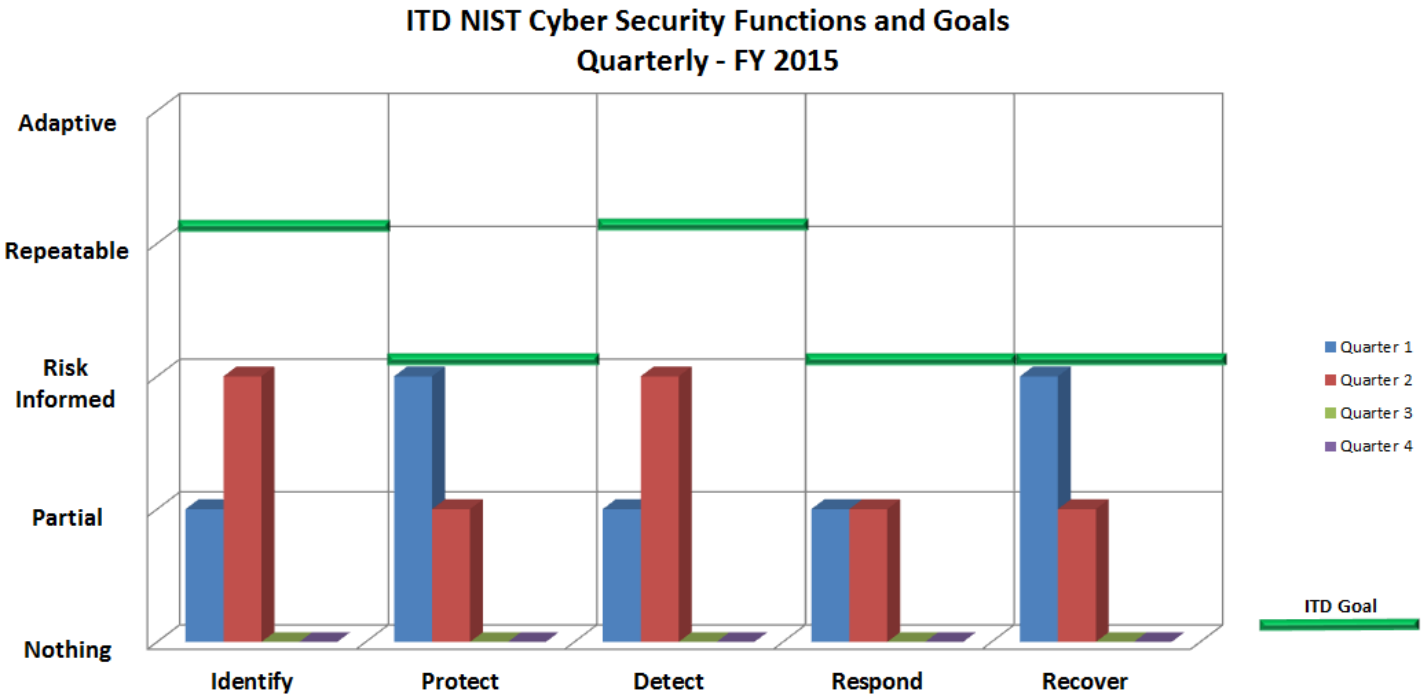
How we metricized the NIST Framework

- Charts
  - We created visual charts to display our metrics
    - Goals and current status. By Function, By Category and by Sub Category.



How we metricized the NIST Framework

- Set Goals
  - We took a look at the difference between our baseline and where we wanted to be and totaled the number of Tiers of improvement needed to reach our goals and spread them over a 3 to 5 year window.



How we use the NIST Framework for Metrics

- We brought in an auditor who specializes in IT from our internal Audit group for a neutral outside view.
- We evaluate the framework quarterly.
- We take notes during the evaluation process. This shows us what our thoughts were during the last round and highlights what we can do to improve.

How we use the NIST Framework for Metrics

- To remove the subjective nature of some of the subcategories we started scoring each control and averaging (with traditional rounding) the score to build the sub category. This is painfully slow at first but can really time in the end because key controls are reused in multiple sub categories. This also shows us some of the most important controls to focus on.

How we use the NIST Framework for Metrics

- We only plan on doing a detailed review once a year and the quarterly reviews based upon changes (completing projects, new threats emerging, how things went)

Lessons Learned

- As a group, we are capable of having very impassioned but detailed discussions on the subject.
- Our baseline was fairly optimistic.
- Sometimes scores drop. Sometimes scores drop because we get a better understanding of what is needed and what we are doing. Sometimes they drop because of the moving target nature of cyber security.

Lessons Learned

- The projects we were working on at the time focused on things we were already strong on, not on the things we were weak.
- This is a group sport. Most of the controls evaluated by the NIST are performed by IT groups outside of IT Security. To reach our security goals, we need to work very closely with the other IT Groups.

Questions?

Email: brian.reed@itd.idaho.gov

NIST: http://www.nist.gov/cyberframework/