Update on the Key Initiatives Recommended by NTT Data regarding the Agency Cyber Security Framework

60x30TX

Texas Higher Education Coordinating Board

Zhenzhen Sun
Assistant Commissioner
Information Solutions and Services

John House
Information Security Officer
Information Solutions and Services

AOC – January 24th, 2018

Implementation Strategy and Approach

- The assessment report produced by NTT Data described the agency's current cybersecurity posture.

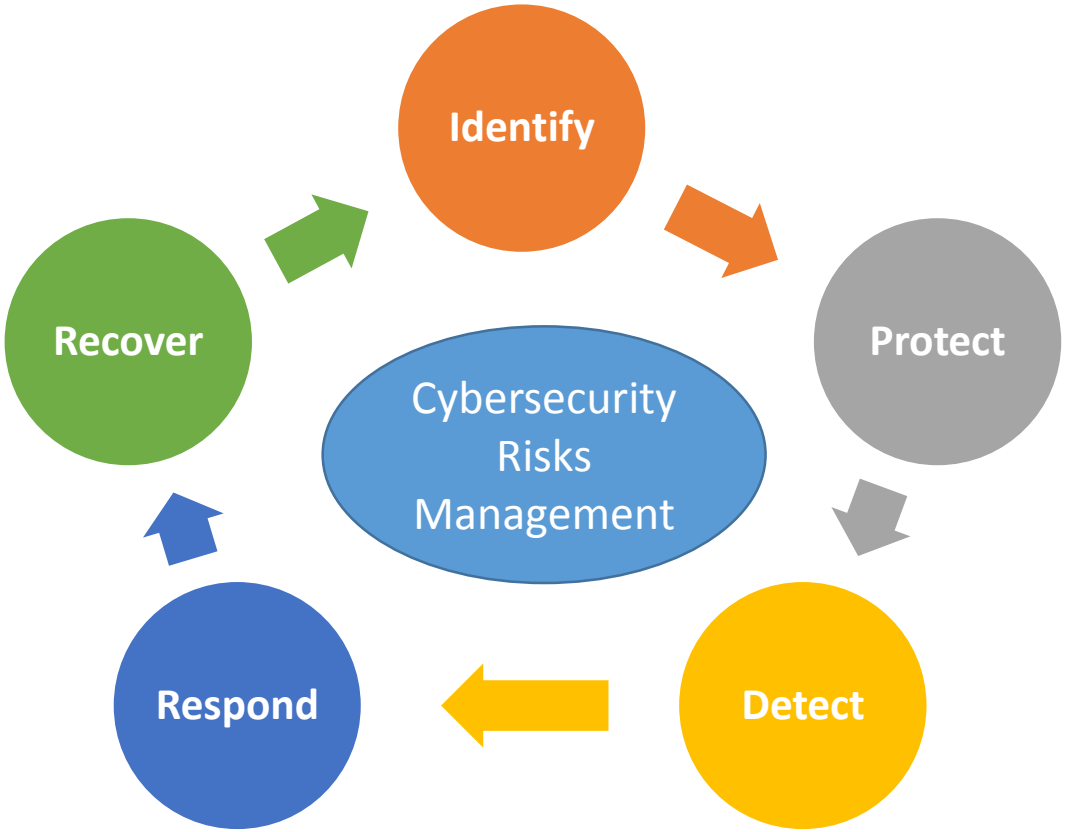
- The recommendations provided by the vendor laid out a "Target State" vision for our cybersecurity infrastructure.

- Our implementation strategy was established by focusing on the five key functions in cybersecurity risks management as outlined in the TX Cybersecurity Framework:
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover

- We assess progress toward the "Target State" on a quarterly basis and make adjustments when necessary.

Cybersecurity Risks Management Framework

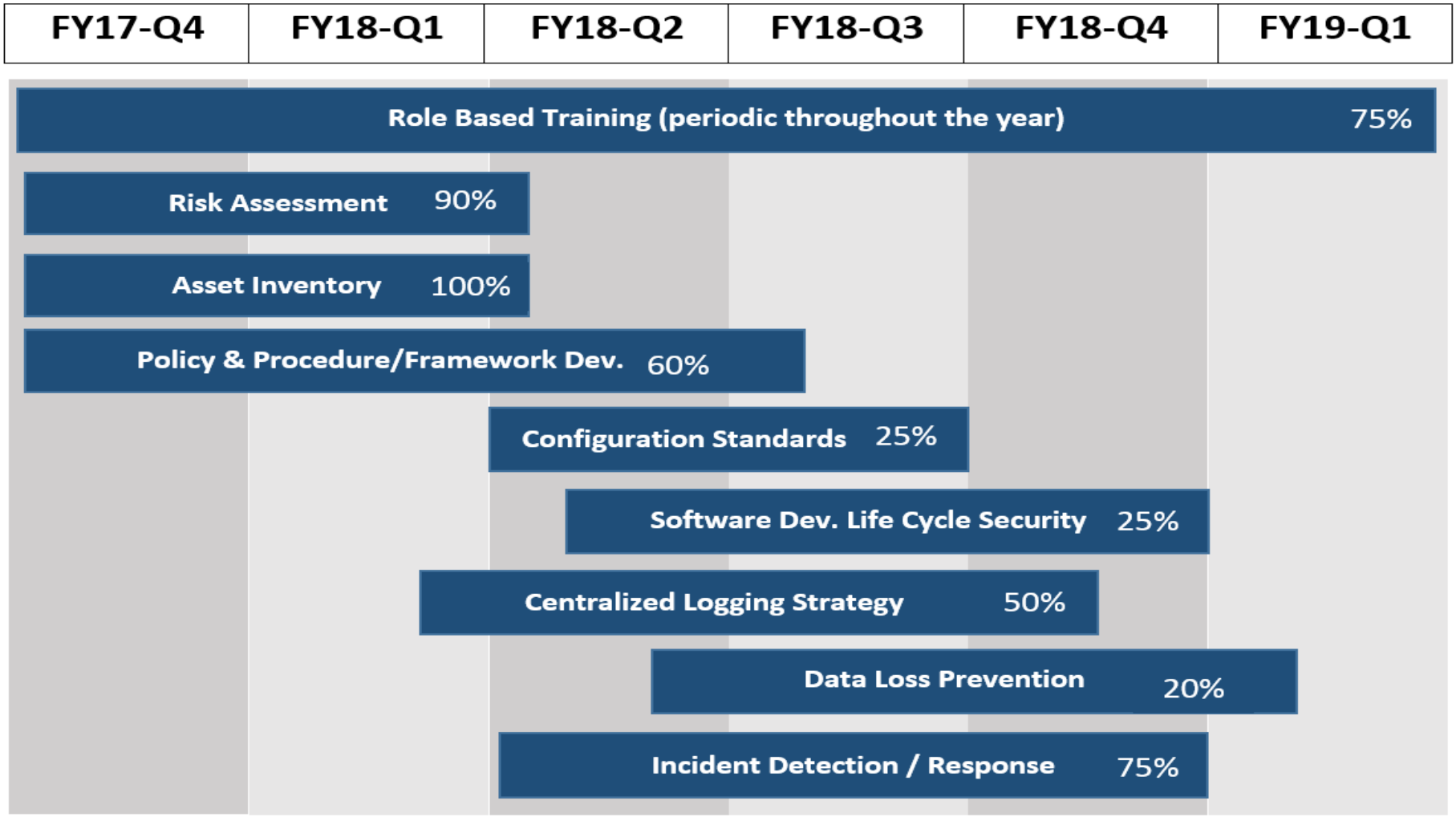
People



Process

Technology

Security Key Initiatives Implementation Roadmap



Progress Report – FY18 Q2

Initiative		Completed	Planned
Protect Role Based Training	75%	FERPA Sensitive PII Training CJIS Training Data Owner Responsibilities Computer Incident First Responder	Application Security Training USB Encryption Training Information Security Training Library
Identify Risk Assessment	90%	Application & Data Inventory Department Review sessions Data Owner Training	Formal presentation to management
Identify Asset Inventory	100%	Risk Assessment Data Inventory USB Survey	Additional USB Inventory Removable Media technical controls
Protect Policy & Procedure / Framework Development	60%	Procedures Updated ITSC Charter Updated IT Policy Review	Additional Security and Application Development Procedure Updates
Protect Configuration Hardening Standards	25%	System Security Plan Template	Complete System Security Plans based on Risk Assessment priorities

Progress Report – FY18 Q2

Initiative		Completed	Planned
Respond Incident Detection & Response	75%	Established Incident Response Team Response Plan updates Quarterly meetings Incident response training	Privacy incident policy and procedures Response Plan exercises
Protect Software Development Lifecycle Security	25%	Web Application Firewall implementation	Updated testing tools Updated coding standards & frameworks Security training for developers
Detect Centralized Logging Strategy (SIEM)	50%	Installed Open Source Security Incident & Event Monitoring (SIEM)	Commercial SIEM / Managed Security Services
Detect Data Loss Prevention	20%	Removable device survey USB Inventory	Additional technical survey and controls for removable devices

Progress Report – FY18 Q2

Identify

- Established a formal Information Security Program
  - ❑ Security Governance Structure
  - ❑ Information Security Charter
- Established a formal agency Security Risk Assessment Tool
  - ❑ Risk assessment results documented and reviewed with management
  - ❑ Agency Application and Data Owners reviewed and verified the risk profile and identified data relationships
  - ❑ Collected an *agency-wide data and systems inventory*
- Currently developing additional removable media device controls and inventory process
- Draft 2017 Agency Risk Assessment and Management Plan pending for review and approval

Progress Report – FY18 Q2

Protect

- Completed updates to 9 security-related policies and procedures
- Using results gathered from the risk assessment to prioritize documenting and the implementation of configuration hardening for agency critical assets
- Currently reviewing and completing system security plans for critical systems identified by the risk assessment
- Provided training to agency staff pertaining to protection of Personally Identifiable Information
- Provided training to Application and Data Owners on owner roles and responsibilities according to the Texas Administrative Code (TAC) 202
- Staff completed Criminal Justice Information Services (CJIS) training
- Updating Application Security Framework documentation
- Currently developing training for the application developers
- Conducted annual review of the agency IT policies and made sure policies and procedures are kept up to date

Progress Report – FY18 Q2

Detect

- Formally established the ISS Computer Incident Response Team
  - ❑ The team completed first responder training in order to strengthen our agency's ability in response to security events and incidents
- Implemented a leading open source Security Incident & Event Management product to provide event monitoring prior to managed services offerings
- Evaluating application security scanning tools offered under DIR Managed Security Service Contract
- DIR Managed Security Services offerings will be evaluated for Security Incident & Event Monitoring offerings

Progress Report – FY18 Q2

Respond and Recover

- Formally established the ISS Computer Incident Response Team
- Implemented the THECB Security Incident Response Plan
- The Incident Response Team will have quarterly meetings and conduct tabletop exercises starting January, 2018
- Working with General Counsel on drafting the Agency Data Breach Policy
  - ❑ Assess, contain and recover data
  - ❑ Assess risk and incident scope
  - ❑ Notification and incident communications
  - ❑ Post mortem evaluation and response

Texas Higher Education Coordinating Board