ALASKA NATIVE
TRIBAL HEALTH
CONSORTIUM

OUR VISION:

Alaska Native people are the healthiest people in the world.

Information Security Program Development

ANTHC IT Security

Presentation Overview

- NIST CSF Approach to Security Program Development
- Cybersecurity Program Document Creation
- Open Discussion, as time allows

Cybersecurity Program: NIST CSF Approach

- Establishing or Improving a Cybersecurity Program
  - Step 1: Prioritize and Scope
  - Step 2: Orient
  - Step 3: Create a Current Profile
  - Step 4: Conduct a Risk Assessment
  - Step 5: Create a Target Profile
  - Step 6: Determine, Analyze, and Prioritize Gaps
  - Step 7: Implement Action Plan

Step 1: Prioritize and Scope

- Identify business/mission objectives and high-level priorities
- Determine assets that support business objectives and priorities
- Align cybersecurity implementations to support business line or process
- Risk tolerance may vary based on business line
- Risk tolerances can be reflected in CSF Implementation Tier

Step 2: Orient

- Identify related organizational assets
  - Devices
  - Applications
  - Data
- Determine regulatory requirements
- Establish overall risk approach
  - Accept, transfer, avoid, reduce
- Identity threats and vulnerabilities applicable to organizational assets

Step 3: Create a Current Profile

- Determine current state
- Develop current profile by indicating which CSF subcategory outcomes are being achieved
- Example profiles:
  - https://www.nist.gov/cyberframework/examples-framework-profiles

Step 4: Conduct a Risk Assessment

- Conduct an internal risk assessment
  - Use threat intelligence to understand current threat landscape
  - Determine likelihood and impact of specific cybersecurity event
  - Start with qualitative analysis
- Center for Internet Security Risk Assessment Method (CIS RAM)
  - Provides a good template for implementing CIS Controls
  - Can be adapted for CSF subcategories (controls)
- Third-party risk assessment
  - Adds credibility and impartiality
  - Intraprise Health's NIST Assessment Platform is a good option

CIS RAM Example

Unique ID	Information asset or asset class	Asset Type	CIS Control Name	CIS Control Number	CIS Control Title	CIS Control Description	How the control is currently implemented	What vulnerabilities are present, given the way the CIS Control is Implemented	What threats could compromise information assets as a result of the vulnerabilities?	How foreseeable is it that this threat would occur and create an impact? Use risk assessment criteria as guidance	What impact could this threat pose to our mission? Use risk assessment criteria as guidance	What impact could this threat pose to our objectives? Use risk assessment criteria as guidance	What impact could this threat pose to our obligations? Use risk assessment criteria as guidance	Risk - Likelihood x Highest Impact Score. Acceptable risk < '9'	Will we accept, reduce, transfer, or avoid this risk?	What safeguard can we use to better implement the CIS Control?	What risk would this recommended control pose to the mission, objectives, or obligations?	How foreseeable is it that this safeguard risk would occur and create an impact? Use risk assessment criteria as guidance	What impact could this safeguard risk pose to our mission? Use risk assessment criteria as guidance	What impact could this safeguard risk pose to our objectives? Use risk assessment criteria as guidance	What impact could this safeguard risk pose to our obligations? Use risk assessment criteria as guidance	Safeguard Risk Score
Risk #	**Information Asset**	**Family**	**CIS Control Name**	**CIS Sub-Control**	**Title**	**Description**	**Current Control**	**Vulnerability**	**Threat**	**Threat Likelihood**	**Mission Impact**	**Objectives Impact**	**Obligations Impact**	**Risk Score**	**Risk Treatment Option**	**Recommended Safeguard**	**Safeguard Risk**	**Safeguard Threat Likelihood**	**Safeguard Mission Impact**	**Safeguard Objectives Impact**	**Safeguard Obligations Impact**	**Safeguard Risk Score**
Example	*Diary device controllers*	*Network*	Wireless Access Control	*15.9*	Disable Wireless Peripheral Access of Devices	Disable wireless peripheral access of devices (such as Bluetooth and NFC), unless such access is required for a business purpose.	*[Supplemented by CIS Control 16.3] Each diary device is joined to the diary device controller using a one-time, six-digit code that is displayed on the controller and entered at the device. At this point, all file transfers and firmware updates are enabled. However, files may only be accessed by devices that use soft-certs that*	*Diary device controllers are using a deprecated version of Bluetooth to support older diary devices. Bluetooth devices with seized soft-certs can manipulate Bluetooth services on the diary device controllers to gain access to files and commands on the*	*Hackers may walk through clinics with Bluetooth devices that are prepared with device-specific soft-certs to hack diary device controllers using attacks such as Blueborne. Hackers must steal soft-certs from diary devices, then guess one-time six-digit codes to access patient files on diary device*	*1*	*3*	*4*	*2*	*4*	*Accept*							*0*

Step 5: Create a Target Profile

- Target profile reflects desired security outcomes
- Informed by risk assessment
- Use to set goals and measure progress
- Roadmap of where you want to be

Step 6: Determine, Analyze, and Prioritize Gaps

- Perform gap analysis by comparing current and target profiles
- Create prioritized action plan
- Benefits of this approach
  - Make informed decisions
  - Supports risk management
  - Perform cost-effective, targeted improvements

Step 7: Implement Action Plan

- Create a plan to address gaps
- Prioritizing is important
  - Trying to close all gaps at once will not work
  - Prioritize your efforts
  - You may need to pivot sometimes, this is okay
- Cybersecurity is not destination, it is a journey
  - Threat landscape is constantly changing
  - Mature programs focus on optimizing their security posture
  - Continual process improvement
  - Evaluate plan at least annually and adjust as needed

Other Uses for Profiles

- Evaluate third party risk
- See CSF subcategory alignment with business mission objectives
  - Helps you to prioritize
- Use to determine gaps in protecting against specific risks
- Use to evaluate implementation of any framework

Other Uses for Profiles, cont.

- Alignment with Business Mission objectives
  - Determine CSF categories most critical to support business mission objectives
  - Easy to understand
  - Helps in prioritizing effort
  - Compare against current profile
  - Informs target profile
- Risk Management Profile
  - Flexible approach
  - Adjust as needed
  - Identify applicable CSF categories
  - Prioritize risk mitigation activities

Example: Alignment with Business Mission Objectives

		Maintain Human Safety	Maintain Environmental Safety	Maintain Quality of Product	Maintain Production Goals	Maintain Trade Secrets
Category		Subcategories				
ID	Asset Management	ID.AM-1	ID.AM-1	ID.AM-1	ID.AM-1	ID.AM-1
		ID.AM-2	ID.AM-2	ID.AM-2	ID.AM-2	ID.AM-2
		ID.AM-3	ID.AM-3	ID.AM-3	ID.AM-3	ID.AM-3
		ID.AM-4	ID.AM-4	ID.AM-4	ID.AM-4	ID.AM-4
		ID.AM-5	ID.AM-5	ID.AM-5	ID.AM-5	ID.AM-5
		ID.AM-6	ID.AM-6	ID.AM-6	ID.AM-6	ID.AM-6
	Business Environment	ID.BE-1	ID.BE-1	ID.BE-1	ID.BE-1	ID.BE-1
		ID.BE-2	ID.BE-2	ID.BE-2	ID.BE-2	ID.BE-2
		ID.BE-3	ID.BE-3	ID.BE-3	ID.BE-3	ID.BE-3
		ID.BE-4	ID.BE-4	ID.BE-4	ID.BE-4	ID.BE-4
		ID.BE-5	ID.BE-5	ID.BE-5	ID.BE-5	ID.BE-5
	Governance	ID.GV-1	ID.GV-1	ID.GV-1	ID.GV-1	ID.GV-1
		ID.GV-2	ID.GV-2	ID.GV-2	ID.GV-2	ID.GV-2
		ID.GV-3	ID.GV-3	ID.GV-3	ID.GV-3	ID.GV-3
		ID.GV-4	ID.GV-4	ID.GV-4	ID.GV-4	ID.GV-4
	Risk Assessment	ID.RA-1	ID.RA-1	ID.RA-1	ID.RA-1	ID.RA-1
		ID.RA-2	ID.RA-2	ID.RA-2	ID.RA-2	ID.RA-2
		ID.RA-3	ID.RA-3	ID.RA-3	ID.RA-3	ID.RA-3
		ID.RA-4	ID.RA-4	ID.RA-4	ID.RA-4	ID.RA-4
		ID.RA-5	ID.RA-5	ID.RA-5	ID.RA-5	ID.RA-5
		ID.RA-6	ID.RA-6	ID.RA-6	ID.RA-6	ID.RA-6
	Risk Management Strategy	ID.RM-1	ID.RM-1	ID.RM-1	ID.RM-1	ID.RM-1
		ID.RM-2	ID.RM-2	ID.RM-2	ID.RM-2	ID.RM-2
		ID.RM-3	ID.RM-3	ID.RM-3	ID.RM-3	ID.RM-3

Example: Risk Management Profile

Category	Subcategory and Selected Informative References	Ransomware Application
Identify		
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 5** CM-8, PM-5	An inventory of physical devices should be undertaken, reviewed, and maintained to ensure these devices are not vulnerable to ransomware. It is also beneficial to have a hardware inventory during the recovery phases after a ransomware attack, should a re-installation of applications be necessary.
	ID.AM-2: Software platforms and applications within the organization are inventoried **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 5** CM-8, PM-5	Software inventories may track information such as software name and version, devices where it is currently installed, last patch date, and current known vulnerabilities. This information supports the remediation of vulnerabilities that could be exploited in ransomware attacks.

Cybersecurity Program Document Creation

- Security Program Composition
- Security Program Structure
- Program Security Components

Security Program Composition

- Purpose and scope statements
- Foundational and supplemental frameworks
  - NIST Cybersecurity Framework (CSF) 1.1
  - NIST SP 800-53 Rev. 5 - Security and Privacy Controls for Information Systems and Organizations
  - NIST SP 800-82 Rev. 2 (ICS) SP 800-82 Rev 3 Draft (OT)
  - NIST SP 800-161 Rev. 1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
- Regulatory Requirements
  - HIPAA
  - PCI/DSS
  - CJIS

Security Program Composition, cont.

- Define your program methodology
  - Overall approach to cybersecurity
- Definitions
- Roles and responsibilities
  - Include security program governance
- Reporting metrics
  - What metrics will you use to track program progress?
- Governance documents
  - Include in program

Security Program Composition, cont.

- Demonstrates overall approach to security
  - No defined format, varies between organizations
  - Focus may change over time based on current threat landscape
- Level of detail may:
  - Explicit
  - Modular
  - Hybrid
- No defined style – it's up to you
- Program security components may be based on:
  - Certified Information Systems Security Professional (CISSP) Domains
  - NIST CSF
  - Regulatory requirements
  - Cybersecurity insurance recommendations
  - Others

Common Security Components

- Training and Awareness
- Vulnerability Management
- Risk Management
  - Third-Party Risk Management
- Incident Response
- Asset Management
  - Devices, applications, data
  - Operational Technology (OT)
- Integration and Coordination

Common Security Components, cont.

- External Attack Surface Management
- Identity and Access Management
- Email and Web Security
- Disaster Recovery and Business Continuity
- Security Assessment and Testing
- Software Development Security
- Policies and Procedures

Example: Training and Awareness

- Three main goals
  - Regulatory compliance – check the box
  - Behavior change
  - Culture change
- Culture change is the desired future state
  - Takes time
  - Requires long-term planning

Example: Training and Awareness, cont.

- Phishing campaign
  - Approach
  - Cadence
  - Enforcement
- Targeted Training
  - C-Level executives
  - Targeted groups (HR, AP)
  - Campus-wide training
  - Needs may vary among departments

Example: Training and Awareness, cont.

- Training resources and schedules
- Integration with organization learning management platform
- Partnerships
  - Human Resources support is key
- Reporting cadence to leadership

Security Component Level of Detail

- Explicit
  - Security Program is longer, but more comprehensive
  - May make it more difficult to revise
- Modular
  - Security Program is shorter
  - More difficult to read
  - May be easier to revise
- Hybrid
  - Approach varies based on security component
  - Most flexible

Importance of Metrics

- Define metrics to:
  - Measure program progress and maturity
  - Quantify effectiveness of cybersecurity program
- Determine how you will communication metrics
  - Determine target audience(s)
  - Reporting cadence
  - Report format – dashboard, data, or both
- Establishing metrics early will simplify reporting later
  - Consider using a spreadsheet that links to multiple views of metrics
  - Edit metrics in one location, configure to replicate to all reports formats

Metric Example

Function	Category	Subcategory	Current	Score
	Asset Management	**ID.AM-1:** Physical devices and systems within the organization are inventoried	ID.AM-1	1
		ID.AM-2: Software platforms and applications within the organization are inventoried	ID.AM-2	5
		ID.AM-3: Organizational communication and data flows are mapped	ID.AM-3	3
		ID.AM-4: External information systems are catalogued	ID.AM-4	5
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	ID.AM-5	1
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	ID.AM-6	2

Support Program by Policies

- Program should be supported by:
  - Policies
  - Standards
  - Procedures
- Relationships between policies
  - Consider using an org chart
  - Easy way to see supporting policies
  - Simplifies spotting gaps

Contact Information

Lorri Booher - ANTHC IT Security

lmbooher@anthc.org

907-317-3147


gunalchéesh • qagaasakung • igamsiqanaghhalek • ‘awa’ahdah • tsin’aen • baasee’ • quyanaa • dogidinh • way dankoo • háw’aa • mahsi’ • maasee’ • chin’an • quyana • quyanaq • quyanaa

ALASKA NATIVE
TRIBAL HEALTH
CONSORTIUM