CONNECT WITH US

Give your Credit Union Direction with the Compass of Critical Security Controls

Disclaimer

The information contained herein has been prepared for general informational purposes only and is not offered as and does not constitute legal advice or legal opinions. You should not act or rely on any information contained herein without first seeking the advice of your legal counsel.

No copy or use of this presentation should occur without the permission of Vizo Financial. Vizo Financial retains all intellectual property interests associated with this presentation. Vizo Financial makes no claim, promise, or guarantee of any kind about the accuracy, completeness, or adequacy of the content of the presentation and expressly disclaims liability for errors and omissions in such content.

"Give Your Credit Union Direction with the Compass of Critical Security Controls Webinar" discussed in this presentation is the current version with effective date of 5/30/2024.

The comments today are my own and not necessarily those of Vizo Financial or the Vizo Financial membership.

Who Am I

VP, Information Security for Vizo Financial

- With the Corporate for 22 years
- Working in Information Technology and Information Security
  - 9 years in Information Technology
  - 13 of those years Information Security
  - GIAC Certified Incident Handler
  - GIAC Security Leadership Certification
  - CompTIA Advanced Security Practitioner

vizo financial

Today's Agenda

Security Frameworks

- What is a security framework?
- Why do we need a framework?
- How does it fit into your program?
- Examples of Frameworks

CIS Critical Security Controls

- Brief overview
- Key Controls to focus on

Questions

What is a security framework?

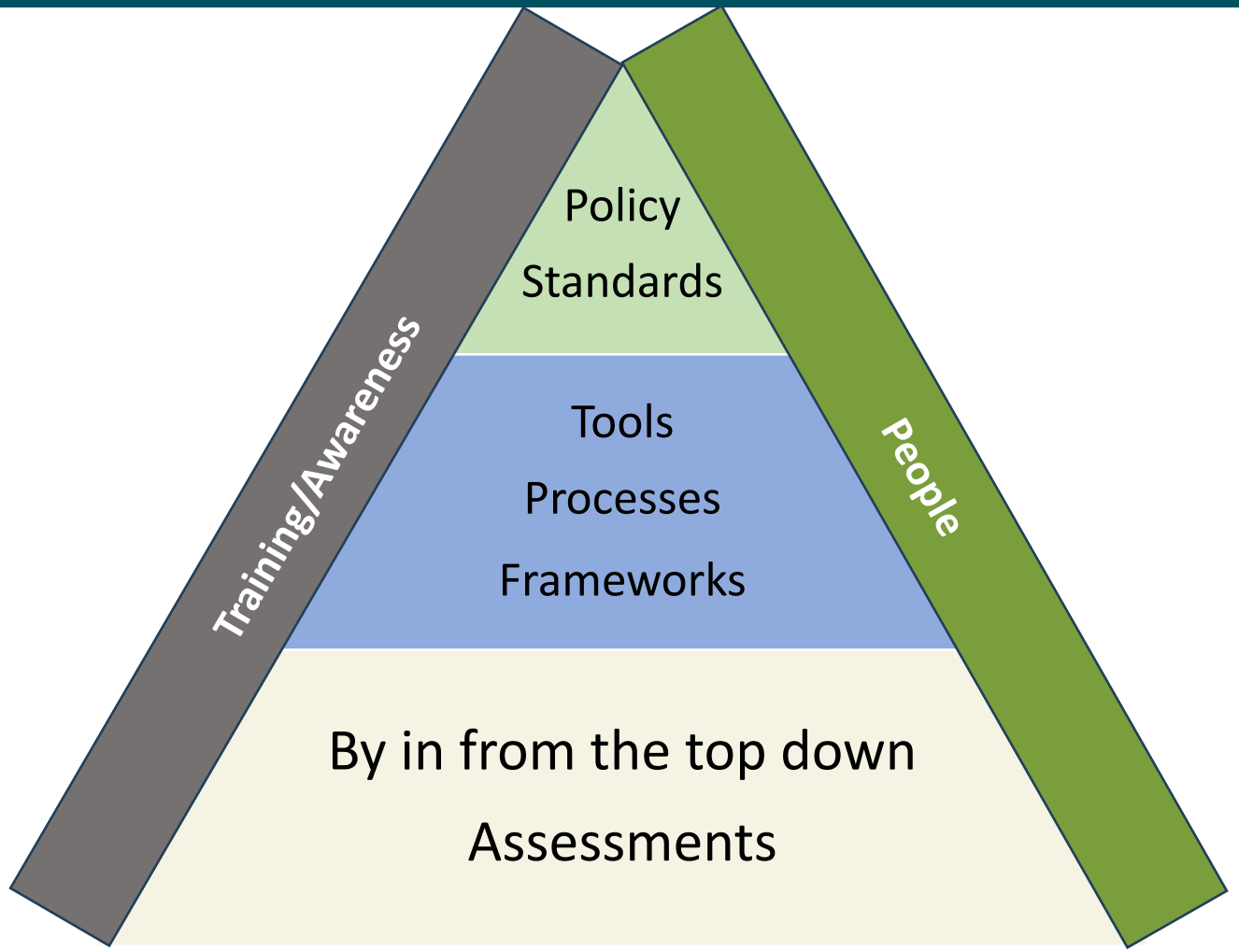
- Frameworks are not…..
  - Required by compliance or regulations
  - Set it and forget it
  - Your entire program
- A security framework is…
  - Guidelines and best practices
  - Designed to help organizations
  - Goal to lower cyber risks

Why do I need a framework?

- Core Tenants of Information Security
  - Confidentiality
  - Availability
  - Integrity

- Core Components of Information Security
  - Assessments
    - Threat
    - Controls
  - Policy & Standards
  - Education
  - Oversight & Reporting

How does a security framework fit into a program?



vizo financial

Examples of Frameworks

- NIST Cyber Security Framework (CSF)
  - v2.0
- ISO 27001 & 27002
  - International Organization for Standardization
- CIS Critical Security Controls
  - Center for Internet Security

vizo financial

CIS CSC

- Center for Internet Security
  - Volunteer Community
    - Information Sharing
    - Create Tools
    - Map Controls to other frameworks
    - Identify and Solve Problems
- Critical Security Controls
  - Best Practices and Recommendations
  - Used by Verizon
  - Top 20 (Now 18)

vizo financial

CIS CSC

- 18 Controls Identified in v8
  - Brief Overview
  - Why
  - Technical Overview
  - Subset of Controls
- Subset are identified
  - 3 Categories
  - Mapped to CSF Function

CIS CSC

- Subset Categories
  - IG1
    - Small to Medium
    - Limited Resources
    - Essentials
  - IG2 (Includes IG1)
    - IT\Security Staff
    - Regulatory Requirements
    - Sensitive Data
  - IG3 (Includes IG1 and IG2)
    - Diverse Security Expertise

CIS CSC

- Critical Security Controls
  - CSC #1 – Inventory and Control of Enterprise Assets
    - Find and track all assets
    - Physically, virtual, remote, and cloud-based assets
    - Address unauthorized assets
  - CSC #2 – Inventory and Control of Software Assets
    - All software
    - Operating Systems
    - Address unauthorized software

Center for Internet Security (CIS) – Critical Security Controls (CSC) v8

vizo financial

CIS CSC

- Critical Security Controls
  - CSC #3 – Data Protection
    - Identify and Classify
    - Retain and Dispose
    - Encrypt end to end
  - CSC #4 – Secure Configuration of Enterprise Assets and Software
    - Hardening standards
    - Maintain and update
    - Implement and manage firewalls

Center for Internet Security (CIS) – Critical Security Controls (CSC) v8

vizo financial

CIS CSC

- Critical Security Controls
  - CSC #5 – Account Management
    - User, Admin, Service accounts
    - Unique Credentials
    - Separate Admin accounts
  - CSC #6 – Access Control Management
    - Request for access
    - Request for removal of access
    - MFA (External, Remote Network, Administrative)

Center for Internet Security (CIS) – Critical Security Controls (CSC) v8

vizo financial

CIS CSC

- Critical Security Controls
  - CSC #7 – Continuous Vulnerability Management
    - Works with asset inventory
    - Hardware and Software
    - Patching Program
  - CSC #8 – Audit Log Management
    - Establish a Standard
    - Collect Logs
    - Retain Logs

Center for Internet Security (CIS) – Critical Security Controls (CSC) v8

vizo financial

CIS CSC

- Critical Security Controls
  - CSC #9 – Email and Web Browser Protections
    - Up-to-Date and Supported
    - DNS Filtering
  - CSC #10 – Malware Defenses
    - Deploy Anti-Malware Software
    - Configure Auto-updates
    - Disable Autorun and Autoplay

Center for Internet Security (CIS) – Critical Security Controls (CSC) v8

vizo financial

CIS CSC

- Critical Security Controls
  - CSC #11 – Data Recovery
    - Process in place to recovery
    - Perform Automatically
    - Protect and Isolate
  - CSC #12 – Network Infrastructure Management
    - Up-to-date
    - Network Diagrams

Center for Internet Security (CIS) – Critical Security Controls (CSC) v8

vizo financial

CIS CSC

- Critical Security Controls
  - CSC #13 – Network Monitoring and Defense
    - SIEM
    - IPS/IDS
    - Manage Remote Connections
  - CSC #14 – Security Awareness and Skills Training
    - Security Awareness Program
    - Social Engineering/Authentication/Data Handling
    - Incidents and Reporting

Center for Internet Security (CIS) – Critical Security Controls (CSC) v8

vizo financial

CIS CSC

- Critical Security Controls
  - CSC #15 – Service Provider Management
    - Establish and maintain an inventory
    - Policy
    - Monitor and Classify
  - CSC #16 – Application Software Security
    - Development Lifecycle
    - Vulnerability Process
    - Training

Center for Internet Security (CIS) – Critical Security Controls (CSC) v8

vizo financial

CIS CSC

- Critical Security Controls
  - CSC #17 – Incident Response Management
    - Designate Personnel
    - Contact List
    - Reporting Process
  - CSC #18 – Penetration Testing
    - Establish a standard
    - External pen tests
    - Process to remediate

Center for Internet Security (CIS) – Critical Security Controls (CSC) v8

vizo financial

Verizon Data Breach List

- Critical Security Controls
  - Secure Configuration of Enterprise Assets and Software (CSC #4)
  - Email and Browser Protection (CSC #9)
  - Malware Defenses (CSC #10)
  - Continuous Vulnerability Management (CSC #7)
  - Data Recovery (CSC #11)
  - Account Management (CSC #5)
  - Access Control Management (CSC #6)
  - Security Awareness and Skills Training (CSC #14)

Verizon 2023 Data Breach Investigations Report - DBIR

vizo financial

Questions