CIS® Center for Internet Security®

The State of Cybersecurity Policy in the US

Focus on State actions and emerging standard of reasonableness

Curtis W Dukes
EVP and GM, Security Best Practices

October 3, 2022

About Me

- Curt Dukes
- EVP & GM Security Best Practices
- Senior Executive NSA
- Infosec, IA, CyberSecurity
- Computer Scientist
- USAF – *Aim High, Fly-Fight-Win*
- Runner, cyclist, old

About CIS

- US-based forward-thinking, non-profit entity that harnesses the power of a global IT community
- CIS Mission:
  - Identify, develop, validate, promote, and sustain best practice solutions for cyber defense
  - Build and lead communities to enable an environment of trust in cyberspace
- MS-ISAC and EI-ISAC are the key resource for cyber threat prevention, protection, response and recovery for the nation’s SLTT and Elections communities respectively
- Create consensus based Security Best Practices

Summary of Federal Action

- H.R. 3684, the Infrastructure Investment and Jobs Act (IIJA) *Public Law No: 117–58 (Nov 15, 2021)*
- H.R. 4346, CHIPS Act of 2022 *Public Law No: 117-167 (Aug 9, 2022)*
- H.R. 2471, Consolidated Appropriations Act of 2022 (including the Cyber Incident Reporting for Critical Infrastructure Act) *Public Law No: 117-103 (Mar 15, 2022)*
- EXECUTIVE ORDER 14028: Improving the Nation's Cybersecurity *(May 12, 2021)*
- EXECUTIVE ORDER 14017: America's Supply Chains *(February 24, 2021)*
- Security & Exchange Commission Regulatory Actions *(Feb and Mar, 2022)*
- TSA Announces Two Security Directives Regarding Rail *(Dec 2, 2021)*
- TSA's Second Security Directive for Pipeline Owners and Operators *(July 20, 2021)*
- Establishment of Cyber Safety Review Board *(February 3, 2022)*
- The Joint Cyber Defense Collaborative *(August 5, 2021)*

State Cyber Security Action

Legislation, Executive, and Judicial Action

- **State Adoption**
  - **Nevada** legislature includes the CIS Controls as a definition of reasonable cybersecurity for state government agencies
  - **Ohio** legislature passes the Data Protection Act that provides legal protections for organizations voluntary implementing the CIS Controls or other defined frameworks
  - **Utah** legislature passes the Data Protection Act, modeled very closely off the Ohio statute
  - **Connecticut l**egislature passes the Data Protection Act, modeled very closely off the Ohio statute
  - **Idaho** Governor's executive order requires executive branch agencies to implement the first 5 CIS Controls
  - **Pennsylvania** court lists CIS Risk Assessment Methodology (CIS RAM), a method that helps organizations assess their security posture against the CIS Controls, as an example of reasonable security test
  - **California** Attorney general warns that failing to implement the CIS Controls "constitutes a lack of reasonable security"

Ransomware Task Force

- Original RTF report called for the need to *"Develop a clear, actionable framework for ransomware mitigation, response, and recovery."*
- Blueprint for Ransomware Defense directly responds to this recommendation.
- An action plan for ransomware mitigation, response, and recovery for small- and medium-sized enterprises (SMEs).
- The Blueprint removes a critical barrier for SMEs with limited resources to defend against ransomware.

Blueprint for Ransomware Defense overview

- A curated subset of *essential cyber hygiene* Safeguards from the Center for Internet Security Critical Security Controls® (CIS Controls®) v8
  - These Safeguards represent a minimum standard of information security for all enterprises and are what should be applied to defend against the most common attacks
- Aimed at small- and medium-sized enterprises (SMEs)
- Comprised of 40 Safeguards – *14 Foundational and 26 Actionable Safeguards*
  - Selected for their ease-of-implementation and effectiveness in defending against ransomware attacks
- Backed by analysis from the CIS Community Defense Model v2.0
  - Implementing the Safeguards in this Blueprint defends against over 70% of the attack techniques associated with ransomware*

*Based on the dataset provided by the CIS CDM v2.0 using the MITRE ATT&CK framework

Blueprint for Ransomware Defense structure

- Seven major areas that are covered in the Blueprint:
  - Know your environment
  - Secure Configurations
  - Account and Access Management
  - Vulnerability Management Planning
  - Malware Defense
  - Security Awareness and Skill Training
  - Data Recovery & Incident Response
- Aligned to the NIST Cybersecurity Framework (NIST CSF) for ease of implementation
- These are actions that should be part of an iterative risk management program at every organization

*Based on the dataset provided by the CIS CDM v2.0 using the MITRE ATT&CK framework

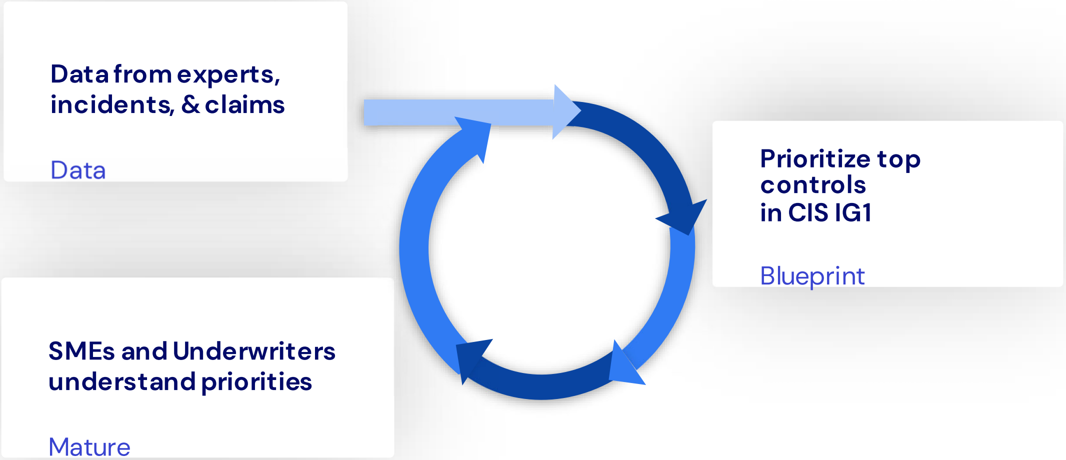
Cyber Insurance

Insurance protected “*industrial economy,*” new approach is needed for “*digital economy*”

- Blueprint “engineering standards” critical shift to a “cyber resilience” approach
- Underwriting based on technical controls -> Share to make insureds safer

Insurance data used to inform prioritization of Blueprint controls

- Based on real data for reducing loss
- Best practices for incident response



Data from experts, incidents, & claims

Data

Prioritize top controls in CIS IG1

Blueprint

SMEs and Underwriters understand priorities

Mature

OSCAL: Open Security Controls Assessment Language

- Set of formats expressed in XML, JSON, and YAML that provide machine-readable representations of control catalogs, control baselines, system security plans, and assessment plans and results
- Goals:
  - Decrease paperwork for assessments
  - Improve system security assessments
  - Enable continuous assessment
- FedRAMP prefers that CSPs (Cloud Service Providers) provide SSPs (System Security Plans) in OSCAL
  - Enable 3PAO automated assessments
  - Expedite Agency review of FedRAMP security authorization packages

Controls and OSCAL

- CIS Controls v8 in OSCAL format
  - https://github.com/CISecurity/CISControls_OSCAL
- Organizations must comply with multiple frameworks
  - Automate mappings/compliance
  - Controls → CSA CCM v4.0
  - *More mappings coming soon (NIST 800-53)*
- Controls Assessment Specification (CAS) ***coming soon***

Why OSCAL?

- Standard way to represent a framework
  - Unique Identifiers survive across versions
- Standard way to represent a mapping
  - Unique Identifier for each mapping survives across versions
- Automate Ingestion of frameworks into tools
  - CSPs
  - Vendors
- Automate mappings of frameworks from authoritative sources

Thank you