(crunchbase, 2021)

TRENDS PRESENTATION: RSA CONFERENCE 2021

KYLER KENT, CISSP

GEORGETOWN UNIVERSITY

ADVANTAGES OF STATUS QUO CYBER GOVERNANCE

- There are many governance plans to choose from
- Tailored governance plans for each situation (e.g., NERC-CIP for electrical providers; HIPAA for healthcare providers).
- Context: regulatory environment, government, military, private sector, etc.

DISADVANTAGES

- Coverage gaps in industry, sector, or business
- Conflicts with each other
- Missing governance approaches

GOVERNANCE TRENDS: FUSION NOT FISSION

- Modern governance trends are moving towards integration and crosswalk with other governance trends
- We have seen this in DODCar/.govcar and MITRE
- NIST Privacy Framework Core and the Framework for Improving Critical Infrastructure Cybersecurity (NIST, 2021).
- NIST Cybersecurity Framework (CSF) to External Dependencies Management Assessment (EDM) Crosswalk (DHS & CISA, 2020)
- Numerous other examples

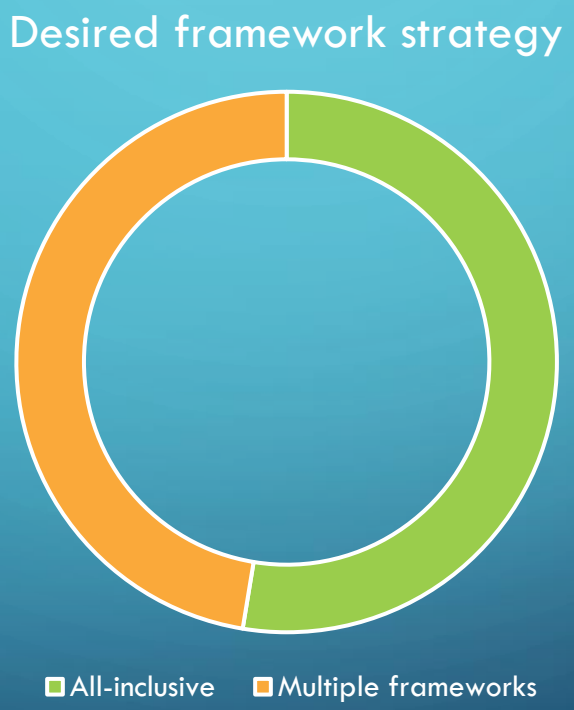
AUDIENCE POLL

A). Would you rather have an all-inclusive framework?

B). Or, would you rather have separate frameworks with adequate crosswalks with each other?

Please text 1 for A or 2 for B to 478134

AUDIENCE POLL RESULTS



EMPIRICAL POST-ANALYSIS

- Let's focus on the desired strategy from our audience
- Inclusivity:
  - DODCar/.govcar
    - Includes:
      - CSF
      - MITRE
        - Everybody loves MITRE
  - ISO 27000 Series
    - Has 60 total standards and covers the "broad spectrum of information security issues" (Kirvan, 2021).
    - Includes cloud, DRP, forensics, evidence, confidentiality, storage, healthcare, and much more (Kirvan, 2021).
  - NIST SP 800 Series
    - Includes "virtually every aspect of information security" (Kirvan, 2021)

EMPIRICAL POST-ANALYSIS CONTINUED

- Inclusivity:
  - New Zealand Protective Security Requirements (PSR) (SecurityScorecard, 2021)
    - Four major categories of security:
      - Security governance (GOVSEC)
      - Personnel security (PERSEC)
      - Information (INFOSEC)
      - Physical security (PHYSEC) (SecurityScorecard, 2021).
    - “32 focus areas” (SecurityScorecard, 2021)

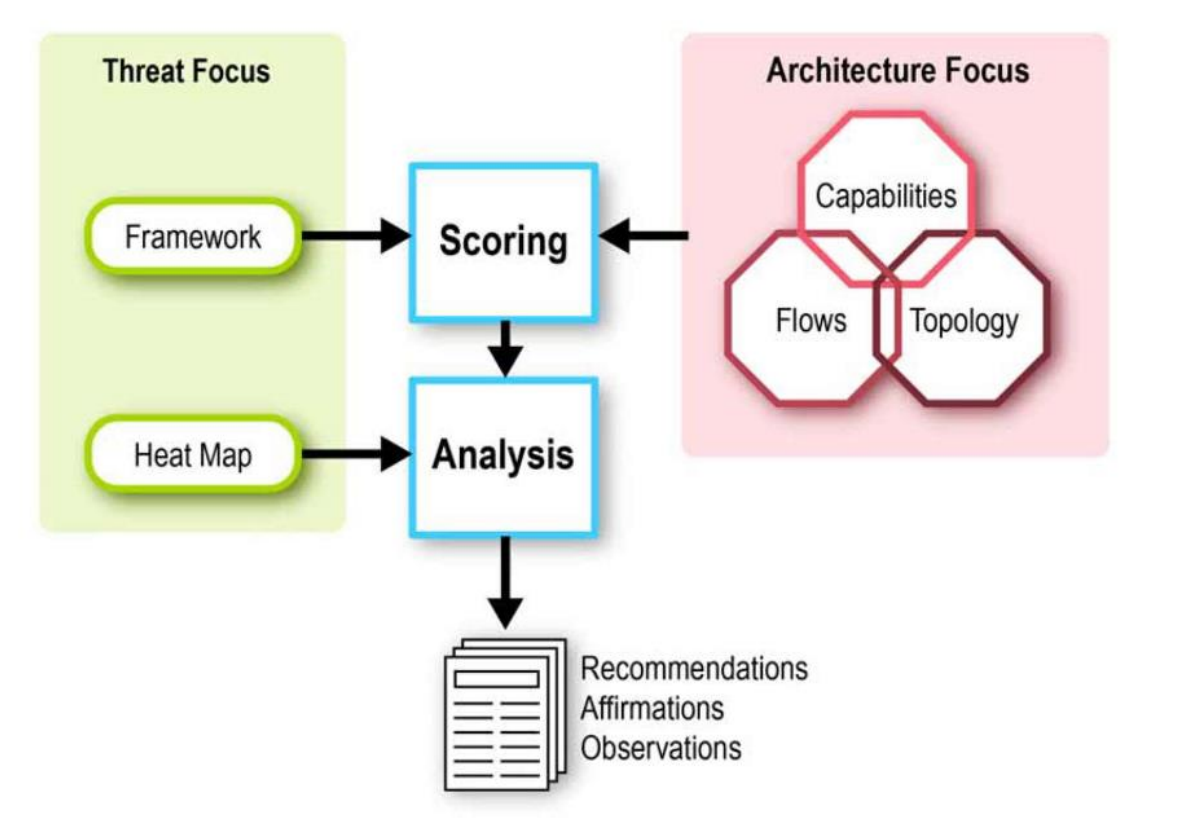
OTHER TRENDS

- Risk-based approach
  - Organizations are moving towards a risk-based approach (Boehm et al., 2020).
  - Unique to the CSF as well as DODCar/.govcar (Kirvan, 2021).
  - Other NIST, risk-based Frameworks:
    - NIST Risk Management Framework (RMF)
    - Factor Analysis of Information Risk (FAIR) Cyber Risk Framework
      - Organizations calculate risk, “regardless of the cybersecurity framework they use” (SecurityScorecard, 2021).

DODCAR/.GOVCAR THREAT-BASED MODEL AND ADVANTAGES

- Threat-based risk management
  - Integrated into the purpose.
  - Built into the framework from the beginning (Department of Homeland Security, 2018, p. 1).
  - Is a part of OMB's movement towards threat-based management (p. 13).
- Advantages:
  - Uses advanced, threat-based technologies like "break & inspect" and integrates them into a broad enterprise strategy (Department of Homeland Security, 2018, p. 14).
  - Focuses on cloud security and architecture
  - Integrates with existing, proven frameworks like MITRE and the CSF (KuppingerCole, 2019).

DODCAR'S APPROACH: COMPREHENSIVE THREAT AND ARCHITECTURE MODEL



(Department of Homeland Security, 2018, p. 4)

DODCAR/.GOVCAR THREAT-BASED MODEL AND ADVANTAGES CONTINUED

- Utilizes a comprehensive formula for calculating cyber risk:
  - "threat * vulnerability * consequence = risk" (Department of Homeland Security, 2018 p. 11).
    - Improves on previous frameworks and takes a MITRE heat map of both threats and "capability coverage" (p. 11).
- Mobile-focused, develops comprehensive control strategy to protect mobile devices (Department of Homeland Security, 2018, p. 9).

DODCAR/.GOVCAR SHORTCOMINGS & IMPROVEMENTS

- Could elaborate more on the cyber risk calculus
  - Could have definitions of each element and how to apply it for an entity.
- Can be narrowly focused on federal agencies.
  - Understandable being a DoD-based framework
  - Could use more broadening like in NIST frameworks to apply to other entities.
  - I am unfamiliar with many of the technologies listed in the framework, despite their goal to be usable by anyone "regardless of their technical background or level of expertise" (KuppingerCole, 2019, para. 5).

QUESTIONS OR COMMENTS?

(Pixabay, 2017)

REFERENCES

Boehm, J., Curcio, N., Merrath, P., Shenton, L., & Stähle, T. (2020, September 16). The risk-based approach to cybersecurity. McKinsey & Company. Retrieved December 4, 2022, from https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-risk-based-approach-to-cybersecurity

crunchbase. (2021). RSA Conference 2021. crunchbase.com. https://www.crunchbase.com/event/rsa-conference-2021

Department of Homeland Security. (2018). DoDCAR/.govCAR Slides. In NIST.gov. COMPUTER SECURITY RESOURCE CENTER. Retrieved December 4, 2022, from https://csrc.nist.gov/CSRC/media/Projects/cyber-supply-chain-risk-management/documents/SSCA/Fall_2018/WedPM2.2-STARCAR%20SCRM%20FINAL%20508.pdf

DHS & CISA. (2020). EXTERNAL DEPENDENCIES MANAGEMENT (EDM): NIST Cybersecurity Framework Crosswalks. In CISA.gov. U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency. Retrieved December 4, 2022, from https://www.cisa.gov/sites/default/files/publications/4_NIST_CSF_EDM_Crosswalk_v3_April_2020.pdf

Kirvan, P. (2021, December 21). Top 10 IT security frameworks and standards explained. TechTarget: Security. Retrieved December 4, 2022, from https://www.techtarget.com/searchsecurity/tip/IT-security-frameworks-and-standards-Choosing-the-right-one

KuppingerCole. (2019). Bringing a Business Perspective to Cybersecurity Operations I. Retrieved December 4, 2022, from https://www.kuppingercole.com/sessions/3497/2

NIST. (2021, April 23). Cybersecurity Framework Crosswalk. Retrieved December 4, 2022, from https://www.nist.gov/privacy-framework/resource-repository/browse/crosswalks/cybersecurity-framework-crosswalk

Pixabay. (2017, March 5). Question Mark on Chalk Board. pexels.com. https://www.pexels.com/photo/question-mark-on-chalk-board-356079/

SecurityScorecard. (2021, November 10). Top 25 Cybersecurity Frameworks to Consider. Retrieved December 4, 2022, from https://securityscorecard.com/blog/top-cybersecurity-frameworks-to-consider