CONSULTING PRESENTATION RE:ARGENTINA

KYLER KENT, KENT INTERNATIONAL CONSULTING INC. Sep 18, 2022

ARGENTINA'S CYBERSECURITY

- Argentina has been a developing country since 1983 (Pollitt, 2008, p. 1537).
- Argentina is currently in 8th place in "country of origin in cyberattacks" (Schreiber, 2018, para. 8).
- Argentina is seeking to create a national cybersecurity strategy with the creation of the "Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad" (para. 19).
- Argentina has "no officially adopted national cybersecurity standards" (Bolgov, 2020, p. 262).
- Argentina is currently "level 2" in its CMM maturity level (Diaz, 2021, p. 42).

(Nurahman, 2019) CC with attribution

RE: ARGENTINA

ARGENTINA IS BEST SERVED BY US NATIONAL CYBERSECURITY STRATEGY

(kjpargeter, 2022) free with attribution

We are a fully developed nation.
We have numerous public and private cybersecurity efforts.
We are a country of origination for numerous cybersecurity governance frameworks as well as organizations.
We set the standards for cybersecurity in the western hemisphere.

US-BASED CYBERSECURITY STRATEGY FOR ARGENTINA

- Embrace unique goals
- Utilize unique framework components
- Federalize adaptive frameworks
- Integrate cybersecurity frameworks with risk management
- Embrace USA's unique "action lines and planned actions" (Luiijf et al., 2011, p. 11)
- Follow US institutionalization

UNIQUE GOALS OF USA'S CYBERSECURITY STRATEGY

- US is focused on protecting critical infrastructure (Luiijf et al., 2011, p. 8).
  - Argentina: Protect the most valuable assets first.
- US wants to decrease "national vulnerability to cyber attacks" (p. 8).
  - Argentina: Focus on lowering the count of vulnerable systems and methods across the country to decrease cybersecurity-related risks.
- US wants to increase cyber resilience (i.e., lower "damage and recovery time") during attacks (p. 8).
  - Argentina: Focus on cyber resilience. Not all threats can be mitigated, especially nation-state actors with almost unlimited resources.

USA UNIQUE FRAMEWORK COMPONENTS

- US is of a handful of nations that identifies each of these parties as stakeholders to "threat, vulnerabilities, and measures:"
  - "Citizens"
  - "SME" (small and medium-sized enterprises)
  - "Large organizations"
  - "CI Operations"
  - "The state/national security"
  - "Global infrastructure & issues"

  (Luiijf et al., 2011, p. 10).
- US is one of three nations that includes international infrastructure in their stakeholder assessment (Luiijf et al., 2011, p. 10).
  - Argentina: take on a global perspective to risk management and business processes.
  - Realize they are one nation in a very large world and need to quickly realize its place in the global community.

FEDERALIZE ADAPTIVE FRAMEWORKS

- US: NIST is authorized and delegated through FISMA to create federal cybersecurity frameworks and standards.
  - Argentina: needs to organize and enforce government cybersecurity standards at the federal level.
- The NIST Cybersecurity Framework (CSF) offers a "flexible way to address cybersecurity" across genres, infrastructures, and contexts (NIST, 2018, p. vi).
  - Argentina: needs to implement NIST or a similar, adaptive framework.
- US: utilizes NIST CSF as "a living document" subject to regular updates, feedback, and improvements (p. vi).
  - Argentina: Needs to tailor NIST CSF or a similar framework to their needs under a lifecycle of improvement.

INTEGRATE CYBERSECURITY FRAMEWORKS WITH RISK MANAGEMENT

- U.S. integrates the CSF with risk management programs (NIST, 2018, pp. 4-5).
  - Argentina: adapt a comprehensive risk management program such as ISO 31000:2009 or NIST SP 800-39 (pp. 4-5)
  - Argentina: integrate the CSF with the risk management program of choice.

"KEY ACTION LINES AND PLANNED ACTIONS" (LUIIJF ET AL., 2011, P. 11)

- US is one of the "only nations explicitly addressing the dynamics of the cyber security threat" (Luiijf et al., 2011, p. 11).
  - Plan for the dynamic nature of cybersecurity threats.
- The US is of a handful of countries with "high-priority," high volume cybersecurity training for military and law enforcement personnel (p. 11).
  - Create well-established government-sponsored training for military and law enforcement personnel.
- The US encourages global partnership with the Cybercrime Convention (p. 11)
  - Foster international partnership and community involvement.

US INSTITUTIONALIZATION

- The USA is a model country for institutionalization with the DHS "Centre of Excellence on Cyber Security" (Luiijf et al., 2011, p. 15).
  - We have been able to make use of pre-existing entities and retrofit them for modern-day threats and challenges (p. 15)
  - Retrofit existing institutions for cybersecurity to organize cybersecurity efforts.
  - This is an economical approach that creates resilient government structures and resilient people. This strategy will support Argentinian economic development moving forward.

REFERENCES

- Bolgov, R. (2020, April). The UN and Cybersecurity Policy of Latin American Countries. In *2020 Seventh International Conference on eDemocracy & eGovernment (ICEDEG)* (pp. 259-263). IEEE.
- Díaz, R. M. (2021). State of cybersecurity in logistics in Latin America and the Caribbean.
- kjpargeter. (2022). *American flag with folds and creases* [Digital Photograph]. freepik, Malaga, Andalucia, es. https://www.freepik.com/free-photo/american-flag-with-folds-creases_918247.htm#query=usa%20flag&position=16&from_view=keyword
- Luiijf, H. A. M., Besseling, K., Spoelstra, M., & Graaf, P. D. (2011, September). Ten national cyber security strategies: A comparison. In *International Workshop on Critical Information Infrastructures Security* (pp. 1-17). Springer, Berlin, Heidelberg.
- National Institute of Standards and Technology (NIST). (2018, April 16). Framework for Improving Critical Infrastructure Cybersecurity. *In https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf* (Version 1.1). NIST Technical Series Publications. Retrieved September 18, 2022, from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- Nurahman, A. (2019, August 20). File:Argentina Flag.png. In *Wikimedia Commons*. https://commons.wikimedia.org/wiki/File:Argentina_Flag.png
- Pollitt, M. (2008). Electricity reform in Argentina: Lessons for developing countries. *Energy economics*, *30*(4), 1536-1567.
- Schreiber, C. (2018). Cybersecurity challenges for Latin America. *Grupo de estudios en seguridad internacional*, *10*.

THANK YOU

KYLER KENT

KENT INTERNATIONAL CONSULTING INC.