WHITE PAPER #4

https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/shutterstock_97535411.jpg

What is the Best Approach for Developing a National Cybersecurity Strategy?

DeBora King

CSIA 360 7980

Cybersecurity in Government Organizations (2172)

May 7, 2017

University of Maryland University College – Spring Semester, 2017

INTRODUCTION

It is in the best interest of all nations to have a plan for uncertainty in a world where the complexities of cybersecurity continue to evolve. This is where national security strategies can help us all. The objective is to provide leadership in protecting the interest of the country's stakeholders. By doing so, the tasks and activities related to mitigating against cyber risks strengthens the nation's security. This is done by using critical teams and collaboration with the public and private sector (White House, 2015). Every nation should have a cybersecurity strategy (including small, resource-poor nations) for many reasons: the potential to strengthen alliances among countries; to level the playing field so that rich countries are not the only powerful source; to promote open markets (partnerships and trade for economic growth); counterterrorism; morality and basic human rights to name a few. The objective of this white paper is to compare and contrast the European Union Agency for Network Information Security (ENISA) guidance document for cybersecurity strategies to a similar document prepared by the and Commonwealth Telecommunications Organization (CTO) approaches to developing national cybersecurity strategies for the cyber policy competition. Both ENISA and CTO serve as a guidance to its members – one to members of States of the European Union and one to members of Commonwealth nations respectively. The best approach for developing a national cybersecurity strategy will also be addressed.

CTO & ENISA COMMON PRINCIPLES & GUIDELINES (SIMILARITIES)

The following chart shows five commonalities between the ENISA and CTO guidance documentation.

Common Principles & Guidelines	CTO	ENISA
Key Performance Indicators (KPI)	In section 3.1.3 of the CTO documentation, the key performance indicator approach is described as a complimentary component to risks to identified national level outcomes. The document uses an example about using it as a testing the level of trust for online businesses.	In section 4.2 of the ENISA documentation, two approaches are listed for using KPI's – one being as a whole and the other activities-driven. National risk assessment is an item that each member state is encouraged to conduct. The document goes on to address each phase KPIs may include.
Incident Response - Computer Emergency Response Team (CERT)	Under section 4.7.5 of the CTO documentation, the CERT network is mentioned as a supporting mechanism for incident response. The document encourages countries to establish a mechanism such as this one to exercise crisis management.	CERTs are mentioned throughout the ENISA documentation. In particular, section 3.14 which addresses establishing an incident response capability outlines tasks that should be mandated or required for CERTs protecting and handling data and establishing workgroups.
Identifying Stakeholders	Under section 4.5 of the CTO documentation, it is recommended that the	Under section 3.4 of the ENISA documentation which is entitled 'Develop a clear

	cybersecurity strategy identifies and lists its stakeholders. The document discusses the collaborative efforts among stakeholders and gives an example of law enforcement working with internet service providers (ISPs) to investigate criminal activity. Listing stakeholders could bring ease to emergency response.	governance structure,' it recommends defining who is ultimately responsible for managing and evaluating the strategy, it also encourages covering stakeholders involved from a broad spectrum. From individual roles and responsibilities to CERT and an advisory body is addressed.
Developing User Awareness	In section 4.7.3 of the CTO documentation, broadly generating awareness is highly encouraged to protect user experience online for the general public. Their objective in this section is to protect the users' rights and responsibilities	Section 3.11 of the ENISA documentation addresses vulnerabilities for individual and corporate users. Factors of security breaches and other vulnerabilities are mentioned, and a list of programs are listed that support user awareness.
Evaluation	Monitoring and evaluation is outlined in section 4.8 of the CTO documentation. It is incorporated into the KPIs section, as it is used for measuring the method in which data is collected. The responsibility of stakeholders is also addressed in this section.	Section 4.1 of the ENISA documentation discusses an evaluation approach. There are different methodologies mentioned in evaluating a strategy. It lists various tasks as a guide to approach the evaluation process ending with the reporting of the status of affairs.

In addition to the commonalities above, both documents offer examples throughout their guidelines in addition to a glossary at the end and additional resources of other nations with strategic strategies.

UNIQUE ASPECTS OF THE CTO PRINCIPLES AND GUIDELINES

The CTO documentation has a table which outlines its Commonwealth Cybergovernance Principles. It outlines the following principles and lists supporting documentation for its purpose (CTO, 2015):

1. Principle 1: “We Contribute to a safe and effective global Cyberspace”
2. Principle 2: “Our actions in Cyberspace supportr broader economic and social development”
3. Principle 3: “We act individually and collectively to tackle cybercrime”
4. Principle 4: “We each exercise our rights and meet our responsibilities in Cyberspace”

The illustration of a risk-based approach to delivering a national Cybersecurity strategy is unique to the CTO documentation, as it gives a clearly defined depiction of how the cycle works with strategic national goals and its components (global and national context, cyberspace threats, important assets and services, commonwealth principles, and cybermaturity assessment) is associated with risk assessment, including the implementation and monitoring of KPIs.

Appendix 5 in the CTO documentation is a very important component. It is often referenced at throughout the document, and the chart lists strategy components, aspects to consider, and example text from published strategies and best practice. These guideline serves as a quickly accessible and, easily readable resource for its members.

UNIQUE ASPECTS OF THE ENISA PRINCIPLES AND GUIDELINES

The ENISA documentation was quite extensive, and the way it lists each item makes the information more understandable for the reader. It has a section in the beginning of the documentation that tells how to use its guidelines, whether it is used as a step-by-step document, added resource, benchmarking tool or maintenance guide (ENISA, 2012). The examples highlighted throughout the document are highlighted in blue. This is a great way for the readers to pinpoint best practices about strategies other nations are using. The highlighted sections also eliminate possible confusion as to what is listed as a guideline and actions or best practices implemented by nations who are exercising their strategy.

National cyber contingency plans (NCPs) are mentioned in the ENISA documentation in addition to critical information infrastructures. This is a section I did not notice in the CTO documentation. It outlines NCP objectives and instructions for its development within a lifecyce.

RECOMMENDATIONS

The items that have been compared and contrasted by each organization are excellent items for best practices for a cybersecurity strategy. In addition to those items, Microsoft has a document of Developing a National Strategy for Cybersecurity (Goodwin & Nicholas, 2013). It includes many of the components mentioned in the CTO and ENISA documents. Like the ENISA document, it puts emphasis on establishing clear properties and security baselines. Without baselines, it would be hard to measure where and how a nation can build on a foundation and/or improvements. Collaboration has also been mentioned in the aforementioned documents. The ITU National Cybersecurity Strategy Guide has a section for World Summit on the Information Society (WSIS). The ENISA guide sums up the structure of their guide using the ‘Plan-Do-Check-Act’ (PDCA) model which can be used for the improvements and practices for

any lifecycle. Finally, it is best to revisit strategic policies every few years to make sure updates are in line with emerging technology.

References:

The White House. (2015, February 6.). Fact Sheet: The 2015 national security strategy. Office of the Press Secretary. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2015/02/06/fact-sheet-2015-national-security-strategy

CTO. (2015). Commonwealth approach for developing national cybersecurity strategies. Retrieved from http://www.cto.int/media/fo-th/cyb-sec/Commonwealth%20Approach%20for%20National%20Cybersecurity%20Strategies.pdf

ENISA. (2012). National cyber security strategies practical guide on development and execution. Retrieved from file:///C:/Users/DeBora%20King/Downloads/ENISA%20Guidebook%20on%20National%20Cyber%20Security%20Strategies_Final%20(5).pdf

Goodwin, C. and Nicholas, J. (2013, October). Developing a national strategy for cybersecurity. Microsoft. Retrieved from file:///C:/Users/DeBora%20King/Downloads/developing_a_national_strategy_for_cybersecurity.pdf

ITU. (2011, September). ITU national cybersecurity guide. Retrieved from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf