A Guideline to Develop National Cybersecurity Framework and Strategy

Settapong Malisuwan

***Abstract*—The fight against cyber crime or cyberwarfare is not of a telecommunications regulator alone, but rather of the government and industry. Given the dynamic and growing sophistication of such cyber crimes and cyber threats, it is impossible to combat such risks with a static information security. As mobile technology and network continues to evolve, so should cybersecurity measures. The role of a telecommunications regulator by the standard of International Telecommunication Union, recommends that regulator must established an early warning system and emergency response to global cyber threats, training and skills development must be provided on various aspects of cybersecurity, a framework must be development for identification, warning and response to such cybercrimes and cyber threats. Cybersecurity is increasingly regarded as a strategic national issue affecting all levels of society. It requires a high-level strategic approach to cybersecurity that establishes national objectives and priorities. It provides a strategic framework for a nation's approach to cybersecurity. This paper proposes a guideline to develop the National Cybersecurity Strategy. The research method is qualitative in-depth interview with many experts in various fields in order to develop a Cybersecurity Framework for Governments. The contributions in this paper could assist government in development of strategy and framework of cybersecurity to protect and foster the digital economy.**

***Index Terms*—Cybersecurity, national, strategy, guideline, digital economy.**

I. Introduction

By 2015, at least 3 billion people, the equivalent of 40% world's total population, had access to the internet, where 45% of internet users are from Asia, compared to over 20% in North and Latin America and 18% from Europe [1]. The soaring internet usage contribution from Asia is entirely because it holds 60% of the world's population [2], making it the next emerging frontier that has potential for tremendous growth from mobile broadband and internet of things.

By the year 2017, it is estimated that mobile broadband penetration will reach 70 percent of the world's total population. By the year 2020, the number of networked devices (the 'internet of things') will outnumber people by six to one, transforming current conceptions of the internet [3].

As mobile data usage and traffic has been increasing rapidly and substantially, far faster than prevention technology referred to as cybersecurity measures and policies, countries worldwide are at a high risk of facing information security challenges more than ever before. The emergence such tremendous cybersecurity threats is due to migration from 2nd Generation and 3rd Generation mobile networks to 4G and then to 5G which is an all IP network, making it prone to cybersecurity threats.

Especially with the emergence of low-cost smartphones and widespread availability of mobile broadband (all IP network), we can expect 99% of users connected to mobile broadband via smartphones by 2020 [4]. In other words, Cybersecurity is no longer a pure computer security issue. Instead, every user connected to internet, via through computers, tablets, smartphones, and Internet of things devices (household appliances) is now prone to risk from cybersecurity. Therefore, it is pertinent that we see cybersecurity as a national policy mater, because the illicit use of cyberspace can have a national wide impact and hamper economic, public health, safety and national security of a country.

Seeing the national wide impact it can have on a country's national security activities, it has should become a priority for governments worldwide to ensure cybersecurity measures and policies are in place, to protect lives and property of their citizens, provide support to businesses and industry sector in ensuring protection against such cybercrimes, and most importantly, national leaders understand the risks and have set measures for protection and mitigation of cybersecurity threats. Nevertheless, a recent 2013 UN study revealed that a significant number of countries are without a national cybercrime strategy [5].

This study contributes by stressing the importance of implementation of proactive strategies, policies and procedures guided by cybersecurity strategy. Most importantly, this research proposes a cybersecurity framework at a national level, as a guideline for governments to devise a cybersecurity strategy and develop policies by taking into consideration all stakeholders perspective, ensuring these policies are a result of a cooperation from local, national and global level [5]. Overall, the aim of this research is to educate the importance of cybersecurity measures and provide a framework for governments and policy makers to mitigate disruption that can be caused by cybersecurity. Bringing together public and private sector stakeholders to build and ensure a resilient cybersecurity posture will also foster economic development.

II. Cybersecurity Strategy and Policy

With the increase in proliferation of mobile broadband connected devices, and technological shift from 2G to 4G, The society has become increasingly dependent on IT. With a shift to 4G it will become dependent on all IP network, this has its benefits in increasing productivity and advancement in

Manscript received July 28, 2015; revised November 30, 2015.

Settapong Malisuwan is with the National Broadcasting and Telecommunications Commission Thailand, Bangkok, Thailand (e-mail: gameooboyxx@hotmail.com).

all industry sectors, yet it also makes the networks more vulnerable to cyber threats.

With advancement in technology, industries, companies and governments have increasingly grown dependent on their IT and putting critical assets on those systems as well. Accordingly, this calls for a need for protection of those critical assets and has become a topic of national interest. Cyber-threats causing a stop in IT services in companies, industries and government institutions can have a major negative impact, putting a hold to services as well as resulting in national security being threatened. Therefore in addition to increasing digital economy readiness for business sectors and government institutions, cybersecurity strategies is also significant, as it has become the most important challenge during the digital economy era.

The extent of cyber risk varies by industry sector, type of business and the level of important of the information asset at risk on the IT network. A more strategic understanding of the value of information asset to the organization's ability to thrive is required, rather than just a focus on the performance of the network or platform. Rapid consolidation and collaboration among organizations means that organizations now operate across multiple sectors and locations. An organization's security framework may be sufficient for its original sector or geography, but expansion calls for security measures to be reviewed in step [6].

The first scare on cybersecurity came since more than two decades ago, thus cybersecurity strategies have surfaced, one of the first countries to recognize the urgency in enacting cybersecurity measures is United States. In 2003 they published the National Strategy to Secure Cyberspace [7]. It was a part of the overall National Strategy for Homeland Security, which was developed in response to the terrorist attacks on September 11th 2001.

In February 2014, the NIST, in United States publically released its framework for Improving Critical Infrastructure Cybersecurity (Framework). The framework provides a methodology to develop cybersecurity measure and strategy within an organization but it does not provide actionable security measures. National Institute of Standards and Technology is a non regulatory federal agency and provides a voluntary framework. Hence, this framework is not compulsory and is not currently a part of the current cybersecurity formal regulation followed by the US. Nevertheless, it is possible that this framework will become the cybersecurity standard supported by federal cybersecurity regulations. There is a growing agreement that this framework is becoming the standard for cybersecurity in US.

On the other hand, there is also no agreement on a common definition of cybersecurity. The lack of common understanding on cybersecurity as a protection against cyber-threats is an obstacle to development of compatible solution at an international level. There also appear to be different views as to what falls within the scope of "national" vs. "private" cybersecurity.

The national cybersecurity strategies influenced by two significant aspects, 1) whether governments perceive Internet as "trusted space" or "distrusted space". 2) Cybersecurity needs a clear scope. Are all notions connected to internet and at risk an aspect of cybersecurity? Data, identity, and/or "essential services" (e.g. electricity distribution).

III. Methodology

The aim of this paper is to propose a guideline to develop National Cybersecurity Strategy. For this research we have conducted in-depth interviews with subject matter experts in areas such as ICT technologies, Academic leaders in Business and Economic aspects, Law, Social Science and current Cybersecurity policy makers in Thailand. There are fifteen experts in various areas as shown in Table I. The conceptual framework of the research is illustrated in Fig. 1.

TABLE I: Interviewing Experts and Area of Expertise

Area of expertise	Numbers
ICT technologies	3
Business and Economic	3
Law	3
Social science	3
Cybersecurity policy	3

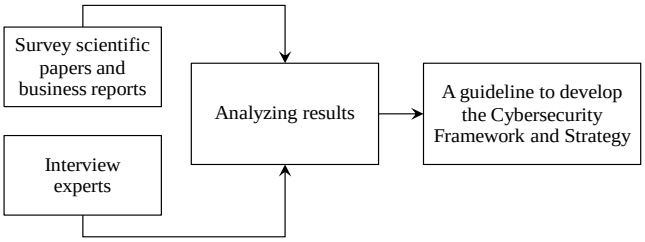

Fig. 1. The conceptual framework of the research.

IV. Results and Discussions

Building an effective cybersecurity strategy can pose many challenges. A document that ticks all the right boxes for what should be included can be easily made. To develop a strategy it is necessary to achieve cooperation and engagement from a wide range of stakeholders on a common course of action. Certainly, this process will be a difficult task. The development team should be realized that the process of developing the strategy is generally as important as the final outcome.

A. Framework

The analysis results from this paper recommended that Cyber Program Management (CPM) framework proposed by reference [8] should be selected as a reference to build the proposed Cybersecurity framework. The basis of this framework takes into consideration the role of information security, IT in businesses and government processes, the level of importance of valuable and information and risk posed if it was leaked, and the overall risk on management structure if under cybersecurity threat. Therefore, this clarifies organization's strategic priorities and organization objectives for both business and government sector.

The research also recommended that the NIST Cybersecurity Framework [9] in conjunction with the CPM from reference [5] is highly recommended as references to build the prototype framework together with other information risk management tools. Finally, this paper proposed the integrated framework from both recommended frameworks as illustrated in Fig. 2.

It will enable organizations of all sizes to effectively demonstrate to stakeholders in building a robust cyber-resilience approach. Hence, the study in this paper can conclude major issues to construct the national cybersecurity.

The framework consists of the following aspects:

1) For an integrated cybersecurity strategy that takes into consideration roles of all stakeholders, the framework must be created through collaboration between industry and government. It must consist of actionable and specific standards, guidelines and practices to promote national security. The framework must adopt a structured approach to understand threats and have specific guidelines for mitigating risks from cyber threats. This will help everyone prioritize and implement important cybersecurity controls faster and with more consistency.
2) The five phases of Cybersecurity Framework are Identify, Protect, Detect, Respond and Recover. This lessens the cybersecurity risks as it organizes information, enables risk management decisions and enable management and mitigation of threats by learning and improving from previous experience.
3) The Cybersecurity Framework will provide a common language in order to ensure coherence in understanding, managing and expressing expressing cybersecurity risk both internally and externally to an organization. The Framework can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk.
4) This framework will be a guideline to enable businesses and governments to understand cybersecurity practices and investments that are in line with specific requirements of each organization. The framework is not suitable but all security activities but is a good starting point for every organization. It is constructed in order to give businesses and governments a direction. In other words, the Framework does not provide a "one size fits all" list of security activities that should be implemented or, for that matter, even a specific list of essential security controls that should be a baseline starting point for every organization.
5) The Framework provides a methodology to think through and develop a cybersecurity program within an organization – it is not the solution itself. Simplistically, the Framework is almost like a GAP analysis
6) The development of this framework integrates principles from many other existing cybersecurity and risk management standards which include the NIST SP 800 series, COBIT, ISO/IEC, and the Critical Security Controls (CSC). However, as cybersecurity threat changes in nature or if the intensity increases or decreases, it is advised for this paper to continue to be developed and improved as industry provides feedback on implementation. As the Framework is put into practice, lessons learned will be integrated into future versions. This will ensure it is meeting the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats, risks, and solutions.
7) During the design process of the Cybersecurity Framework, the designers should consider the questions below.

How can the Preliminary Framework:

1) adequately define and address outcomes that strengthen cybersecurity and support business objectives?
2) enable cost-effective implementation?
3) appropriately integrate cybersecurity risk into business risk?
4) provide the tools for senior executives and boards of directors to understand risks and mitigations at the appropriate level of detail?
5) enable senior executive awareness of potential consequences of successful cyber attacks?
6) provide sufficient guidance and resources to aid businesses of all sizes while maintaining flexibility?

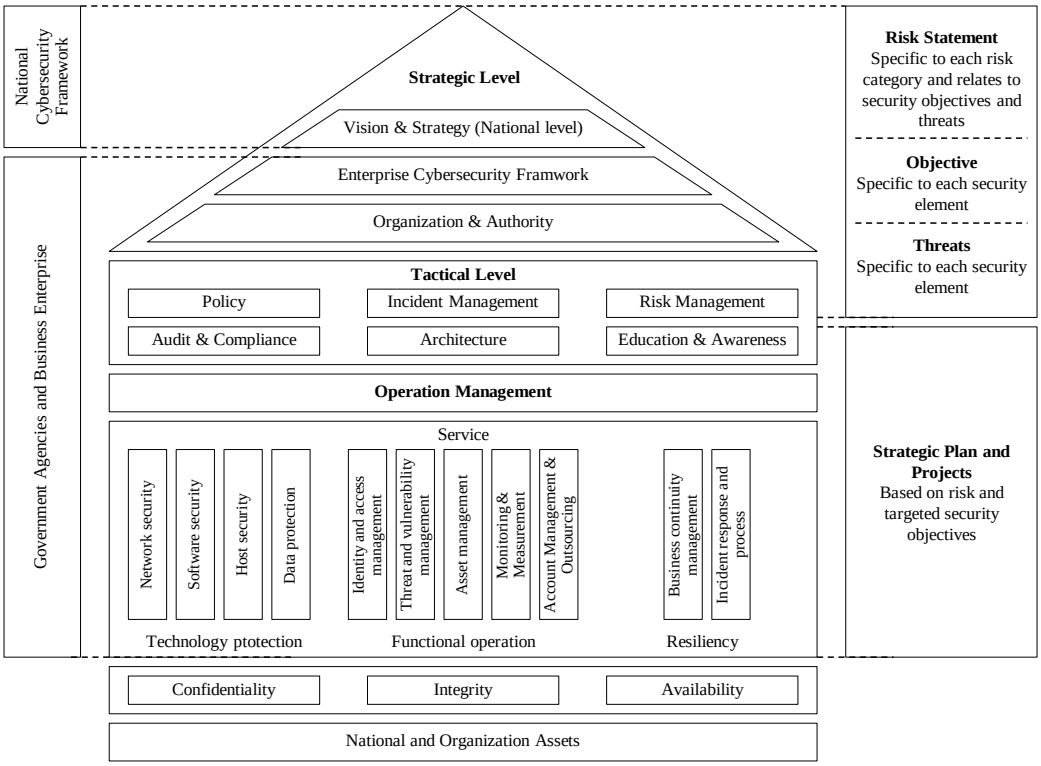

Fig. 2. Integrated cybersecurity framework.

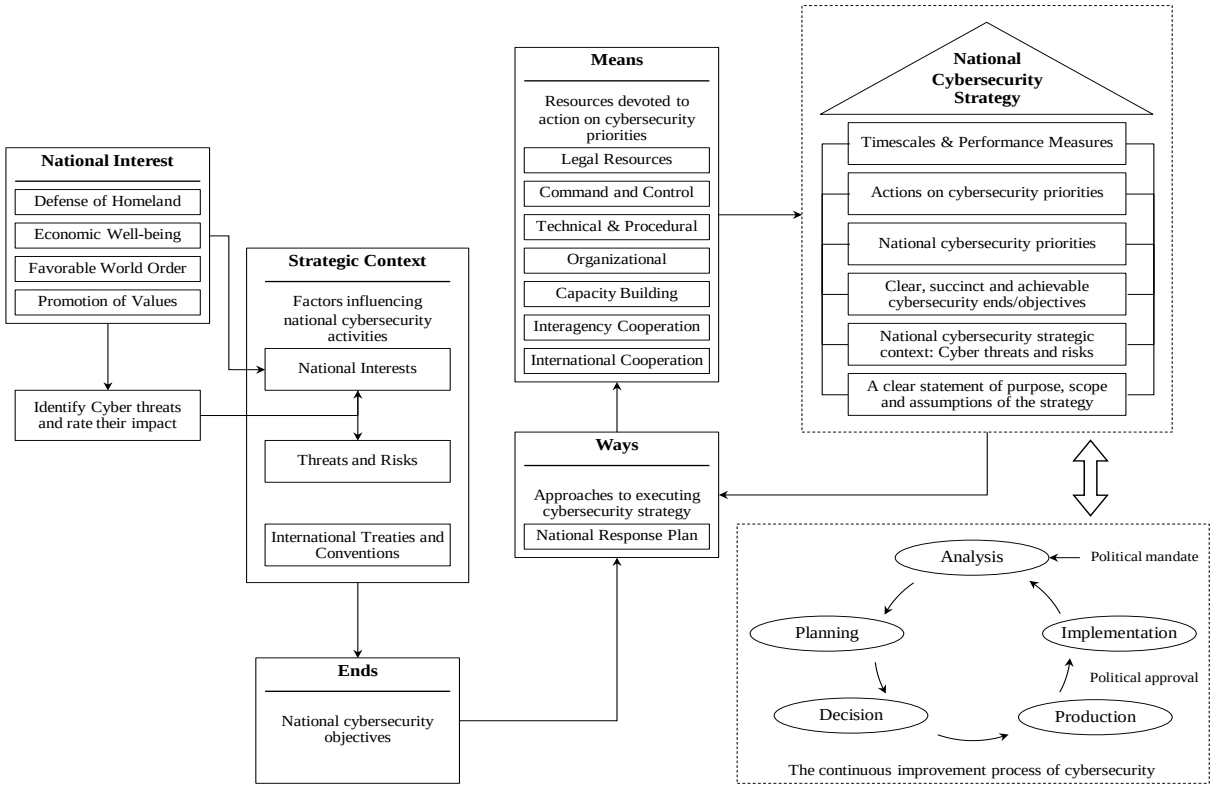

Fig. 3. National Cybersecurity strategy model (modified from [8]).

B. Strategy

The objective of the national cybersecurity strategy is to achieve a continuous improvement approach which will make it possible to more efficiently and effectively implement cybersecurity measures. The strategy process manifests itself at several levels and it includes different phases. The goal is to create a continuous strategy process with parts that regularly repeat and generate continuous improvement. In this research, the continuous improvement process of cybersecurity is integrate into the modified Ends-Ways-Means cybersecurity strategy model to complete the our proposed model as shown in Fig. 3 [5].

The results of the research also provides key cyber risk management concepts as follows: [10]

Include cyber risks into existing risk management and governance programs.

1) Put forward cyber risk management discussions to the top level managers and CEO.
2) Focus on industry standards and best practice
3) Evaluate and then quickly react and be proactive in managing organization's specific cyber risks.
4) Trial and test cyberthreat response plans and procedures.
5) Coordinate cyber incident response planning across the enterprise.
6) Maintain situational awareness of cyber threats.
7) Proactive and efficiency in dealing and reacting to cybercrime, adequate cross–border provisions are needed, and international cooperation and mutual assistance within law enforcement needs to be enhanced [11].
8) Businesses must have proactive measures to manage cyber threats and fast and effective response strategies. They should plan for, protect against, detect and respond to cybersecurity incidents as shown in Fig. 4. Table II shows the detail of proactive measure of cybersecurity. Cyberattacks cannot be foreseen but increase in efficiency to limit damage is significant [6].

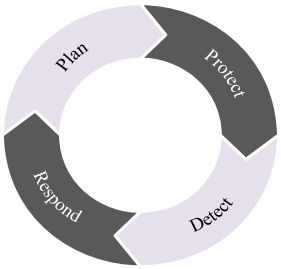

Fig. 4. Proactive measures of Cybersecurity [6]

TABLE II: PROACTIVE MEASURE OF CYBERSECURITY

Measure	Action
Plan	• Assess environment • Identify and remediate gaps • Develop incident response plan
Protect	• Harden environment • Improve authentication • Manage privileged accounts • Limit unnecessary communication • Potentially reduce user privileges
Detect	• Network security monitoring program in place - not just IDS • Key network egress points monitored • Logs archived and analyzed • Key host information collected
Respond	• Computer Incident Response Team (CIRT) staffed and trained • CIRT chartered with authority to drive response • Response and remediation cycle times are measured

1) Organizations must develop strategy to detect ad mitigate potential cyber attacks. Research should be

conducted to understand the nature of cyberthreats that need protection against.

2) Must efficiently manage cybercrime, coordinate with neighboring and cybersecurity crossborder institutions. Must also ensure mutual understand of cybersecurity and strategies and laws are consistent with of region and other neighboring countries.[10].

C. Recommendations

The results of the research gave recommendations as follows:

1) To strengthening security systems, the government should open a dedicated cybercrime center. Meanwhile, the government has to continue to seek new opportunities for international co-operation.
2) Information security agencies have to work with policymakers to take a broad view and to treat attacks on computers and infrastructure the same way. The government should not separate the protection of infrastructure from the applications that run on top of it.
3) The government should collaborate with telecom sector, banking, transport, and public sectors to adopt risk management measures and to report significant incidents to competent authorities.
4) Cybercrime conducted in one application, could provide access to other applications the user uses. Therefore it is borderless in naure and makes cybercrime investigations more complicated for law enforcement authorities. To effectively tackle cybercrime, adequate cross–border provisions are needed, and international cooperation and mutual assistance within the region law enforcement needs to be enhanced.
5) The government must understand that the Cybersecurity framework is a living document that helps an organization define their current and desired cybersecurity state, identify areas of need, and how well they are progressing in that direction, as well as advice on how to communicate to internal and external stakeholders about risks that threaten services.
6) Cybersecurity is a global issue, it is no longer just a single business or single country issue. Therefore, it requires cooperation from governments and industry alike to recognize cybersecurity as a shared global problem. Hence, the government must encourage all stakeholders consider doing the following:
   - Revise security policy documents to adopt and reflect the language and vocabulary of the framework.
   - Establish regular procedures for identifying new threats, testing security procedures, and updating procedures to address those threats, thereby establishing an adaptive cybersecurity program.
   - Ensure that senior management is active in establishing a cybersecurity strategy for the company and reviewing the implementation of that strategy.

V. Conclusion

Cybersecurity has become a vital national security issue that requires tremendous attention and planning to mitigate risk it has on nations and even regions. The aim of this paper is to provide a guideline to draw up a Cybersecurity Framework for governments to follow. However, cybersecurity is not a single country of specific company issue. All stakeholders including governments and industries need to recognize the urgency of protection against cyberthreats. Hence, an analysis of trends in cyberthreats, best practices in protection and the level of international coorperation required must be done to address not just present but future challenges.

The major objective of this research aims to propose a guideline to construct the National Cybersecurity framework. This guideline aims to provide useful and practical recommendations to relevant public and private stakeholders on the development, implementation and maintenance of a cybersecurity strategy. More specifically the guide aims to: define the areas of interest of a cybersecurity strategy; identify useful recommendations for public and private stakeholders; help countries to develop, manage, evaluate and upgrade their national cybersecurity strategy; contribute to the Commission's efforts towards an integrated international cybersecurity strategy. The guide describes: a simplified model for developing, evaluating and maintaining a national cybersecurity strategy.

Cybersecurity planning and implementation efforts must extend far beyond security and IT personal to include all stakeholders such as business owners and governments but must include the cooperation at a regional and international level.

References

[1] Internet World Stats. (2015). Internet Users in the World Distribution — 2014 Q4. [Online]. Available: http://www.internetworldstats.com/stats.htm
[2] World Population Statistics. (2014). Asia population 2014. [Online]. Available: http://www.worldpopulationstatistics.com/asia-population-2013/
[3] UN, "Comprehensive study on cybercrime," UNODC, Vienna, 2013.
[4] Cisco, "The internet of everything and the connected athlete: This changes everything," 2013.
[5] F. Wamala, *ITU National Cybersecurity Strategy Guide*, 2011.
[6] Ernst and Young, *Get Ahead of Cybercrime*, 2014.
[7] The White House Washington, *The National Strategy to Secure Cyberspace*, 2003.
[8] ITU, *Guidelines for the Preparation of National Wireless Broadband Master Plans for the Asia Pacific Region*, 2012.
[9] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*. 2014.
[10] Homeland Security, *Cybersecurity Questions for CEOs*, 2014.
[11] EuRActiv. (2012). Cybersecurity: Protecting the digital economy. [Online]. Available: http://www.euractiv.com/infosociety/cybersecurity-protecting-oil-internet-linksdossier-508217#group_positions

Settapong Malisuwan was born on March 24, 1966 in Bangkok, Thailand. He was awarded full scholarship from Thai government for PhD in electrical engineering (telecommunications), specializing in mobile communication systems from Florida Atlantic University, State University System of Florida, Boca Raton in 2000. He received his MSc degree in electrical engineering in mobile communications system from George Washington University in 1996 and was awarded the First Class Honors, Gold Medal Award and Outstanding Cadet Award by the university. He also got an MSc degree in electrical engineering in telecommunication engineering from Georgia Institute of Technology in 1992. Furthermore, he achieved military education from Special Warfare Center, Thailand, specializing in Ranger and Airborne Courses in 1989 and 1988 respectively. He is currently the Vice Chairman and Board Commissioner of National Broadcasting and Telecommunications Regulator in Bangkok, Thailand. He was awarded the "Science Towards the Excellence in 2013" by The Senate Standing Committee on Science, Technology, Communications and Telecommunications. His research interests are in electromagnetics, efficient spectrum management and Telecommunications policy and management.