An Approach for the Development of National Information Security Policies

Fahad T. Bin Muhaya
MIS Department, College of Business Administration
Prince Muqrin Chair (PMC) for IT Security,
King Saud University (KSU), Riyadh, Saudi Arabia
fmuhaya@ksu.edu.sa

Abstract: *The security of the cyberspace is both a national and an international issue concerned with different levels including: people, enterprises, and governments. It is also associated with different activities including: technical, economic, social and political. As a result, interest in the development of sound national information security policies is becoming of increasing importance. This paper aims at providing a comprehensive approach for this development. For this purpose, the paper is divided into two main parts: the first reviews key related issues in order to establish the necessary background for the work; while the second describes the target approach. The approach has four main dimensions: a structured scope that integrates all the issues concerned; a development process that deals with responding to security requirements on continuous basis; security measures and standards for assessments and benchmarking; in addition to past experience and knowledge sharing for improvements. It is hoped that the approach will become a base for the development and continuous improvement of a national information security policies, not only for Saudi Arabia, but also for other countries in different parts of the world.*

Keywords: *Information Technology (IT); Information Security; Information Security Policy; IT Security; National Information Security Policy; International Standards; STOPE: Strategy, Technology, Organization, People, Environment Framework.*

1. Introduction

As this paper is concerned with providing an approach for the development of national information security policies, the first part of it introduces basic concepts associated with the subject; and it addresses key related issues from different sources distributed over different parts of the world. These key issues include: views from Saudi Arabia; the recent national information security plan of the USA; the "OECD: the Organization of Economic Cooperation and Development" issued principles of information security, recommended for its member countries, and the "ISO: the International Standards Organization" information security management standards. In considering these issues, this first part of the paper establishes the background upon which the target policy development approach is based.

Basic concepts: "Security policy" is defined by the ISO as "an approved top level statement, with a set of rules or plan of action, for the purpose of maintaining appropriate security for the organization" [ISO 2002], where the organization here may range from a small enterprise to a country, a group of countries, or even the whole world. "Information security" is also defined

by ISO as "preservation of Confidentiality, Integrity, and Availability (CIA) of information; in addition, other properties such as: authenticity, accountability, non-repudiation, and reliability can also be involved" [ISO 2005]. Furthermore, ISO defines "information technology (IT) security" as "the protection resulting from an integrated set of safeguards designed to ensure the confidentiality of information electronically stored, processed or transmitted; the integrity of information and related processes; the accountability of information stored, processed or transmitted; and the availability of systems and services" [ISO 2002].

The above ISO definitions illustrate that in the digital age, "IT security" is an integrated part of "information security", and that "security policy" is a prerequisite for protecting both. In the current information age, information associated with all fields of life is being primarily stored, processed and transmitted using IT, and forming, with the prominent IT tool the Internet, what is widely referred to as the "cyberspace". Information security, in this practically open for all space, is becoming increasingly threatened, and this is placing a challenge on all fields of human activities and at all levels, from the personal and family level to the national and international levels, as shown in Figure 1.

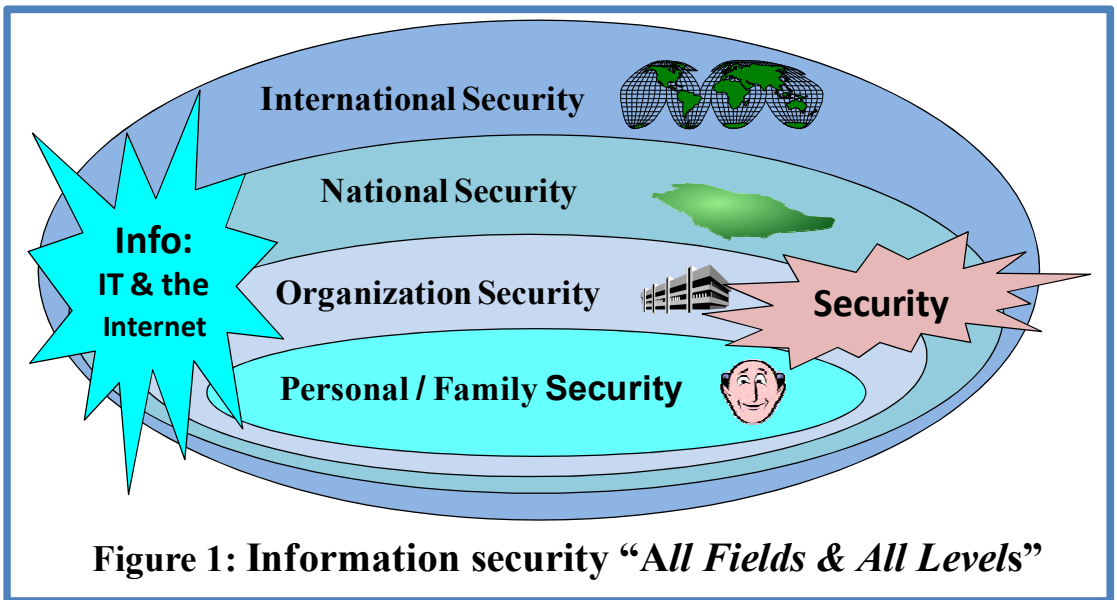

Figure 1: Information security "A*ll Fields & All Levels*"

Saudi views: In Saudi Arabia, concern in information security has been rising. In an interview, on the occasion of the "Conference of Information Technology and National Security" held in Riyadh in December 2007, Prince Muqrin bin Abdulaziz Al-Saud presented views that integrate IT and information security with the various national security dimensions concerned with the protection of people and the safeguarding of the various national activities, associated with the economic, social and political dimensions [Al-Saud 2007]. These views are illustrated in Figure 2; they stress that the protection of information and information technology is essential to all dimensions of life and to international cooperation and competitiveness.

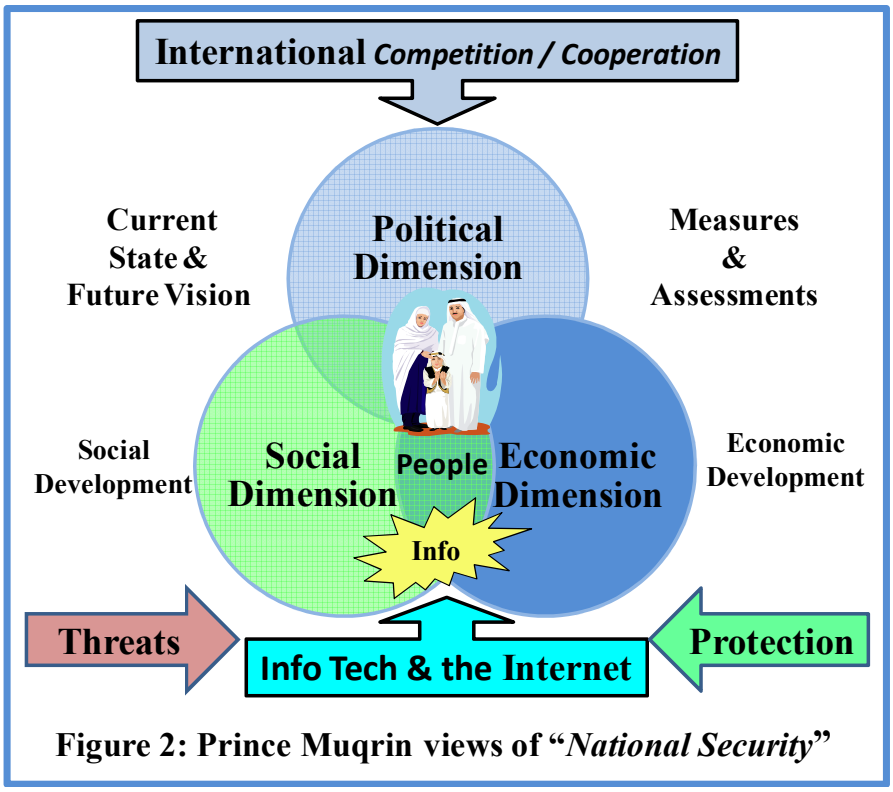

Figure 2: Prince Muqrin views of "*National Security*"

USA plan for information security: In December 2008, the US "CCIS: Center for Strategic and International Studies" issued a report entitled "Securing Cyberspace for the 44th Presidency" [CCIS 2008]. In May 2009, the 44th US President Obama issued a statement emphasizing the importance of the US cyber-security policy given in the report [Obama 2009]. The policy addresses the need to work on "nine main issues" in order to deal with the cyber-security problems.

- One issue addresses "leadership", and considers that it is centered in the "White House" due to the special importance of the problem.
- Another issue is concerned with "strategy", and in this respect DIME should be taken into account, that is: Diplomacy; Intelligence; the Military, and the Economy.
- Two issues are associated with "cyberspace regulations" and "modernization of authorities".
- One issue considers "previous work" of others and the need not to re-start over; while another emphasizes "cooperation" between public and private sectors.
- Two issues address the development of "product acquisition policy" and the "authentication of digital identities".
- The final issue is of course not the least important; it stresses capabilities and considers research and development.

Figure 3 illustrates the above "nine main issues".

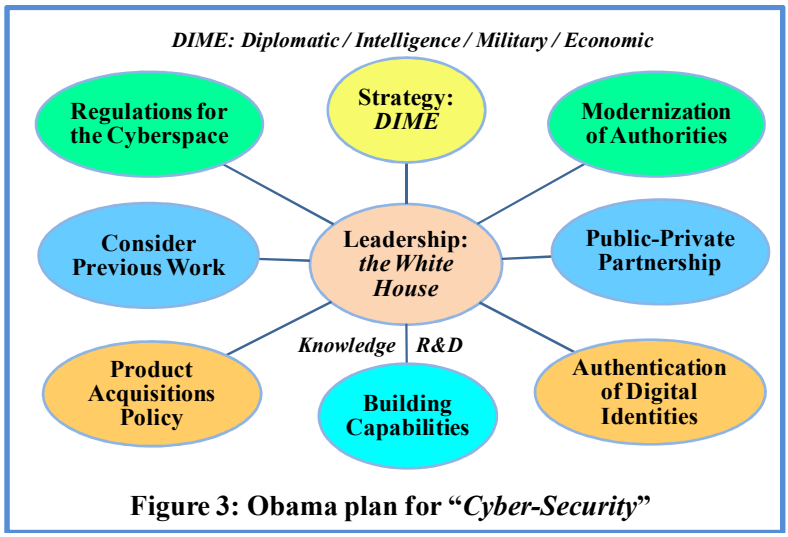

Figure 3: Obama plan for "*Cyber-Security*"

OECD Security of Information Systems and Networks: OECD is an organization of mainly developed countries concerned with "economic cooperation and development". In 2002, it issued "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security" [OECD 2002]. The guidelines have been recommended to OECD member countries. One important part of the guidelines is "the principles" upon which the guidelines are based. As shown in Figure 4, "nine principles" have been considered, and these can be viewed as associated with three groups.

- One group gives three general features, that is: "responsibility, awareness and response".
- Another group considers ethical and other related issues including "ethics and democracy".
- A third group is related to technical practices including: "risk assessment and re-assessment"; and "security design and management".

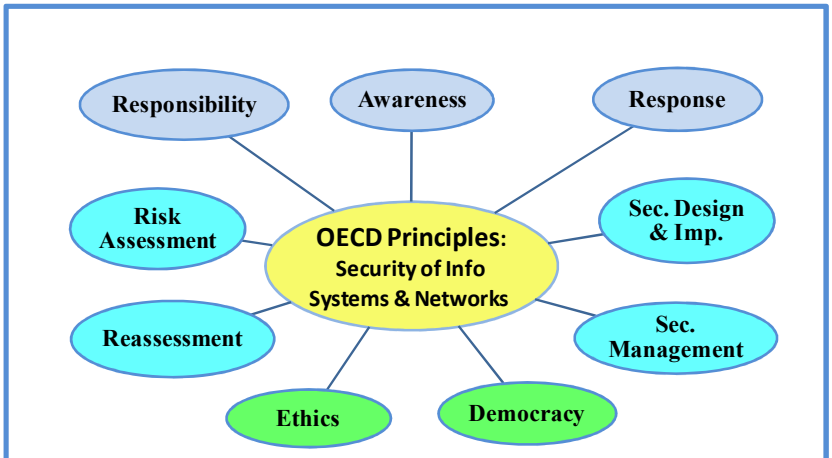

Figure 4: OECD principles of security "*info. systems & networks*"

ISO International Standards: ISO issued two widely known information security standards advocating the need of organizations for "information security policies". These are ISO 17799 [ISO 2005 a] and ISO 27001 [ISO 2005 b] which are concerned with the "code of practice" and "requirements" of information technology security techniques. The ISO policy objective in these standard states the following: "to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations". The contents of these standards have been structured according to the "STOPE: Strategy, Technology, Organization, People and the Environment" scope to ease their comprehension and support their application (Saleh et al, 2007). This is shown in Table 1.

The ISO standards provide two integrated security "directions" for enterprises. The first direction is concerned with their security controls identified as "essential", and these include "21 controls"; while the second is associated with all of their controls, which include "133 controls". The first direction provides an initial standard protection perimeter for security; while the second gives a full standard one. It should be noted here that organizations may increase their security controls further, depending on their requirements.

Table 1: A STOPE view of ISO/IEC 17799 and 27001 contents

STOPE View	Subject	Objec.	Controls	
			Total	Essential
Strategy	Information Security Policy	**1**	**2**	**1**
Technology	Communications and Operations Management	**10**	**32**	**0**
	Access Control	**7**	**25**	**0**
	Information Systems Acquisition, Development and Maintenance	**6**	**16**	**5**
Organization	Organization of Information Security	**2**	**11**	**1**
	Asset Management	**2**	**5**	**0**
	Information Security Incident Management	**2**	**5**	**3**
	Business Continuity Management	**1**	**5**	**5**
People	Human Resources Security	**3**	**9**	**3**
Environment	Physical and Environmental Security	**2**	**13**	**0**
	Compliance	**3**	**10**	**3**
Total objectives and controls		**39**	**133**	**21**

The above has highlighted key information security policy issues at the organization level, the national level and group of countries or international level. All these levels are of integrated nature in the cyberspace. In the following an approach is introduced for the purpose of

supporting the development of national information security policies, hoping that it will be of future benefit to interested countries.

2. Development Approach

The approach concerned with the development of "national information security policies" attempts to incorporate the key issues addressed above in a well-structured and organized manner that eases the task of the development of such policies on the one hand, and supports its outcome on the other. The approach is based on the following main principles.

- To provide a "comprehensive well-structured scope" that enables the incorporation of the various issues concerned.
- To employ a "development process" that supports response to new challenges and new developments.
- To apply acceptable "measures" that assess performance, with support associated with security controls and benchmarks.
- To use "past experience" with "knowledge sharing" that support continuous improvements.

Figure 5 illustrates the above four principles; and the approach is described in the following according to these given principles.

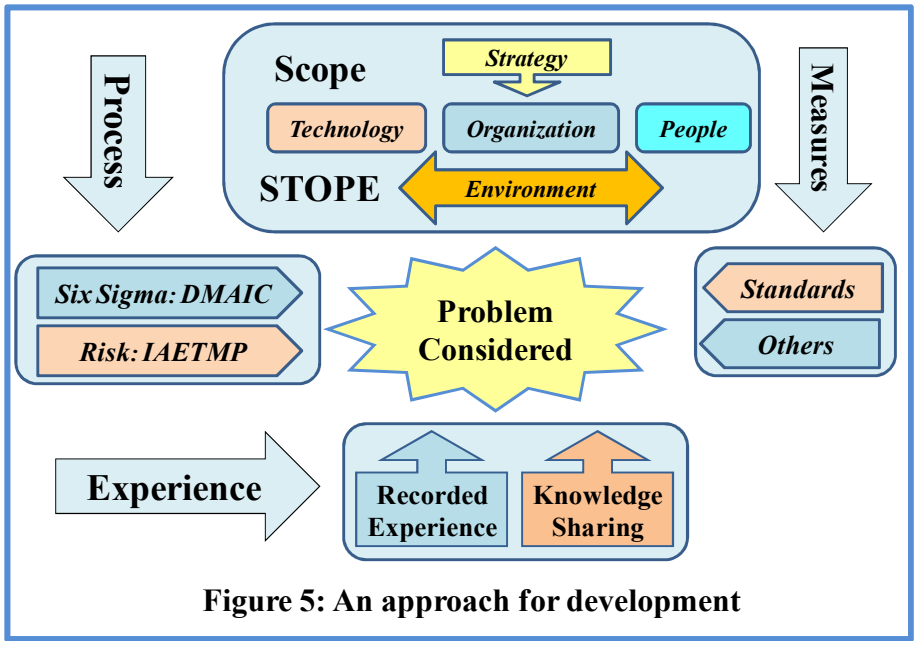

Figure 5: An approach for development

Scope: The approach considers that Bakry's STOPE view as an appropriate scope for the issues associated with national information security policies [Bakry 2003]. The following are some points that illustrate the capabilities of the STOPE domains with regards to the development of the target policies.

- The "strategy" domain would incorporate: the dimensions of Prince Muqrin views; the DIME strategy and leadership of Obama's plan; the various principles of the OECD; and the information security policy of ISO 17799 and 27001.
- The "technology" domain would consider the technology threats and protection measures of Prince Muqrin views; the product acquisition and authentication of

Obama's plan; technology assessments and security designs of the OECD; and the technology aspects of the ISO standards.

- The "organization" domain would be concerned with administrative threats and protection measures of Prince Muqrin views; the regulation and modernization of Obama's plan; responsibility, response and other issues of the OECD principles; and the ISO organization considerations of Table1.
- The "people" domain is at the core of all security requirements as shown in Figure 1; and it is associated with all levels and aspects of threats and protection measures.
- The "environment" domain is concerned with the national and international aspects of both Prince Muqrin views and Obama's plan. It is also associated with the: awareness, ethics and democracy of the OECD principles; and it is related to ISO recommendations.

In the development of national information security policies, all issues concerned can be mapped upon the STOPE domains and their refined sub-domains. It should be noted here that each of the domains may include issues that represent "threats" to security and "controls" for its protection, as illustrated in Figure 6.

Process: The development process needs to be gradually sequenced, systematic and of continuously repeated nature. In this respect two possible processes can be taken into account. One process is the six-sigma "DMAIC: Define, Measure, Analyze, Improve and Control" process [Saleh et al 2006]. The other process is the usual risk assessment and treatment process "IAETMP: Identify, Analyze, Evaluate, Treat, Manage, set or reset Policy". Figure 6 considers the use of this process.

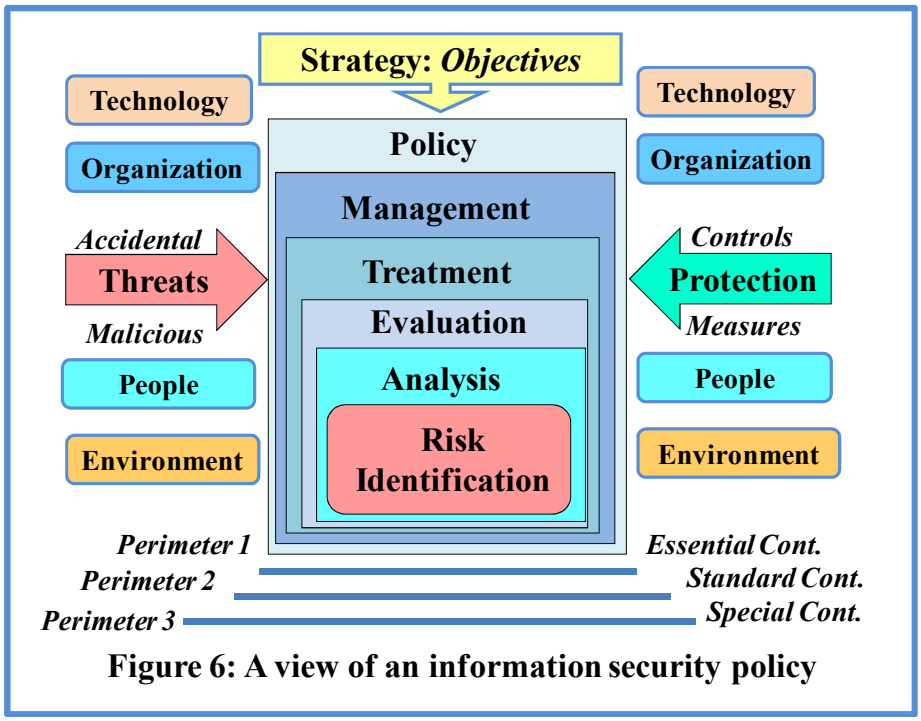

Figure 6: A view of an information security policy

Measures: In security, two types of measures are usually needed. Measures expressed in terms of protection actions and controls; and measures given as assessment tools and

references with benchmarks. Both are needed for performing the phases of the development processes. They are also usually given by ISO standards. It should be noted that in many cases, measures would need to be developed and used in order to match with certain circumstances and requirements. Figure 6 shows that the measures and controls are associated with the protection requirements.

Experience: Obama's plan emphasizes the need not to start or re-start over again and instead to build on past experience and development. In fact experience is usually associated with two sources: recorded experience; and shared experience that can be generated from experienced people. Both are needed and should be prepared for.

National security policies may need priorities in their implementation plans. Considering ISO standards, priorities can be viewed according to three levels, where each level represents a security perimeter, as given in the following.

- Perimeter 1 has the highest priority; and it includes the implementation of essential controls.
- Perimeter 2 has the second priority; and it involves additional controls that take the security up to a proper baseline level.
- Perimeter 3 provides enhanced protection over the previous one, but with relatively higher cost. It is usually needed under special circumstances.

The above perimeters are incorporated with the approach, as illustrated in Figure 6.

3. Future Work

This paper has reviewed key issues concerned with "national information security policies"; and has presented an approach for the development of such policies. The approach has been built upon four pillars: "scope, process, measures and experience". It has provided recommendations on how to deal with each one of these pillars. It can now be used as a tool for the future derivation and improvement of national information security policies in different countries.

The next step for us at Prince Muqrin Chair (PMC), for IT security, is to facilitate the use the approach for building a sound national information security policy for Saudi Arabia. Knowledge on information security needs to be shared among experts in order to enable the proper use of the developed approach and derive of the target well thought policy. For this purpose, PMC is intending to call for a seminar that brings experts together and create the right environment for their contributions. The successful derivation of the target policy would be beneficial to the country, on the one hand; and it would also enhance its leadership position in the region in dealing with a vital and timely problem, on the other.

References

Al-Saud M (2007), An interview on information technology and national security. Conference on Information Technology and National Security, Saudi General Intelligence, Riyadh, Saudi Arabia, Dec. 1-4, 2007.

Bakry S.H. (2003), Development of security policies for private networks, *International Journal of Network Managemen*t, Wiley, Vol. 13, Issue 1, pp 203-210.

CSIS: Center for Strategic and International Studies (2008), *Securing Cyberspace for the 44th Presidency*, CSIS Commission on Cyber-security for the 44th Presidency, December 2008.

ISO (2002), *Guide 73: Risk Management Vocabulary-Guidelines for use in Standards*, International Standards Organization, Geneva, Switzerland.

ISO (2005 a), ISO/IEC 17799: Information Technology-Security Techniques-Code of Practice for Information Security Management; *International Standards Organization*, Geneva, Switzerland.

ISO (2005 b), ISO/IEC 27001: Information Technology-Security-Techniques-Information security management Systems-Requirements; International Standards Organization, Geneva, Switzerland.

Obama B (2009), Statement on Cyber-Security, Office of the White House Press Secretary, May 29, 2009.

OECD: Organization of Economic Cooperation and Development (2002), *Guidelines for the Security of Information Systems and Networks: Toward a Culture of Security*, OECD, 2002.

Saleh M.S., Alrabiah A., and Bakry S.H. (2007) A STOPE model for the investigation of compliance with ISO 17799-2005 *Journal of Information Management & Computer Security*, Emerald, 15(4): 283-294.

Saleh M.S., Alrabiah, A., and Bakry, S.H. (2006) Using ISO 17799-2005 security management standard: A STOPE view with six sigma approach, *International Journal of Network Managemen*t, Wiley, Vol. 17, pp 85-97.