Journal of Computer Science 6 (7): 808-812, 2010
ISSN 1549-3636

Dominant Factors in National Information Security Policies

Fahad T. Bin Muhaya
Prince Muqrin Chair for IT Security (PMC),
Management Information Systems, College of Business Administration,
King Saud University, Riyadh, Saudi Arabia

Abstract: Problem statement: National information security policies are essential parts of the overall national security policies of nations. This study attempted to investigate the dominant factors that need to be addressed in such policies. **Approach:** The study reviewed the national information security policies of different courtiers, focusing on the dominant factors of all of these policies. These factors were compiled and compared in order to determine the common and the non-common policy considerations among these countries. The countries considered include: USA, Malaysia, Australia, Canada and China, in addition to the European Union. **Results:** Recognizing all the common and non-common dominant factors considered by the policies of all the countries considered, the study delivered a generic framework that incorporates all of these dominant factors. **Conclusion:** The resulted generic framework can be used as a guide for the improvement of existing national information security policies in different countries and for the future development of such policies in countries where they do not yet exist.

Key words: National security, national information security, national information security policy

INTRODUCTION

In order to protect their people, organizations and territories, countries usually develop their own national security policies. Such policies should enable their nations to establish a secure threat free environment that supports sustainable development. The policy has to be formulated based on a National Cyber Security Framework (NCSF) that comprises legislation and regulatory, technology, public-private cooperation, institutional and international aspects. The national security policy needs to address the risks to the critical national information which comprises the networked information systems of many critical sectors like National Defense and Security, Banking and Finance, Information and Communications, Energy, Transportation, Water, Health Services, Government, Emergency services, Food and Agriculture (National IT Council, 2010). Cyber security is a distinctively challenging policy issue with an extensive range of public and private stakeholders within countries and outside national boundaries.

The speedy implementation, in some countries, of new information and communication infrastructures, including the Internet, is creating new opportunities for these countries and their citizens to participate in the world's flow of information, ideas and commerce. Multinational corporations are doing business in such countries by outsourcing their work through the easily and widely connected network. But at the same time it initiates new threats and vulnerabilities.

The National Information Security Policy (NISP) is an important part of the national security policy. The NISP provides the starting point of confidence to users. The NISP should be analyzed and assessed for various loop holes. The assessment results help users to make sure whether the information system is secure enough or the potential risk in operation is tolerable. So it's important for critical systems to evaluate their security status (Yan and Shu, 2005).

Every nation has to protect their critical infrastructure from cyber attacks such as such as hacking, email spam, Denial-of-Service (DoS) attacks, virus attacks and cyber terrorism. Nations has to focus on its mitigation to enhance local information security capabilities and develop new skills and competencies. Situational awareness capabilities and contingency planning are important aspects to consider which can be done by building the skillful human recourses.

Cyber security cannot be assured by one person, but is a shared responsibility among all stockholders who are using the communications infrastructure. A key element of effective cyber security policy must be creating the right awareness of and incentives for cyber risk management at all levels: Home computer users, small and large corporations, as well as local and

national governments. This should take the form of complete educational initiatives including encouraging the culture of cyber security best practices in technical practices, risk management practices in business settings and best practices for the home users (Bruce *et al*., 2005).

In this context studying of existing information security requirement against international standards and best practices is of vital importance. Analyzing the existing international security implementation models and determines the possibility to put into operation such model locally for any country. For this purpose information security legislation and regulation are the important milestones. Policy makers, policy implementers and the operations are interlinked to build national policy. The same hierarchy has to be adopted at international, national, sector and firm level depicted in Fig. 1 (Bruce *et al*., 2005).

MATERIALS AND METHODS

The NISP of different countries: Six NISP are reviewed in the following:

United States of America (USA): Identifying the factors considered by a country for its national information security policy is not a straightforward task. According to (American National Security Policy, 2002) national security policy of the USA comprises of the six policy divisions, foreign policy, economic policy, defense policy, energy policy, immigration policy, homeland defense policy. An ongoing discussion is that what are the national and vital interests, who and what threatens them and what should be done about it (American National Security Policy, 2002). Based upon this and some other literatures available like (Bruce *et al*., 2005); the authors can outline the critical factors considered by the USA, which are shown in Table 1.

Information security is not just a study drill. There are risky adversaries out there capable of launching serious attacks on the nation's information systems that can result in severe or catastrophic damage to the nation's critical information infrastructure and ultimately threaten the economic and national security (Ross, 2005). Legislation is very important factor for insuring the national security. The USA has many legislative and policy drivers like:

- Public law 107-347 (Title III)
- Federal Information Security Management Act of 2002
- Public law 107-305
- Cyber Security Research and Development Act of 2002

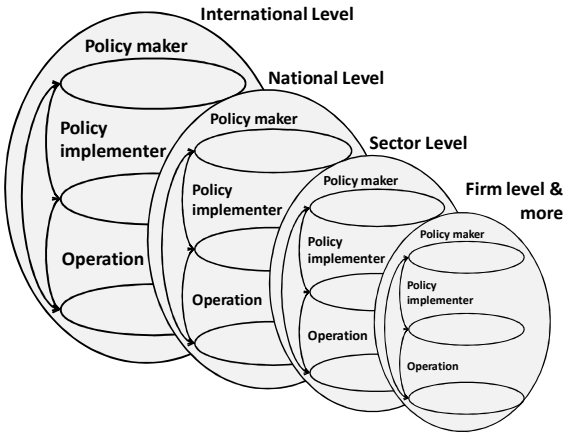

Fig. 1: Overall view of information flows

Table 1: Key factors of the national security (USA)

Sr. No.	Factors
1	Political alliances
2	Military alliances
3	Legislation
4	Law enforcement
5	Cyber Emergency Response Team (CERT)
6	Intelligence agencies
7	Software and hardware vendors
8	Internet service providers
9	Media
10	Computer Security Incident Response Services (CSIRT)
11	Corporate training
12	Academic institutions

- Homeland security presidential directive # 7 critical infrastructure identification, prioritization and protection
- OMB Circular A-130 (Appendix III)
- Security of federal automated information resources

There are very clear directives like Federal Information Security Management Act of 2002 states that "Each federal agency shall develop, document and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source" (Federal Information Security Management, 2002).

Malaysia: Malaysian government and the private sectors have identified the key sectors for the security concern. The key sectors are Military, transportation, banking and finance, health services, emergency services, energy, agriculture, water and information and communication (Rehman, 2002). Some of the key factors considered for the national security are given in Table 2.

Table 2: Key factors of the national security (Malaysia)

Sr. No.	Factors
1	Effective governance
2	Legislative and regulatory framework
3	Cyber security technology framework
4	Culture of security and capacity building
5	Research and development towards self reliance
6	Compliance and enforcement
7	Cyber security emergency readiness
8	International cooperation
9	Information security standards and best practices
10	Cyber Emergency Response Team (CERT)
11	Computer forensic
12	MyCERT: Malaysian Cyber Emergency Response Team
13	Co-ordination and continuity management

Table 3: Key factors of the national security (Australia)

Sr. No.	Factors
1	Legislation
2	Political and military alliances
3	Economics
6	Geopolitics
7	Energy and resources security
8	Impact of climate change
9	Industry
10	Technology
11	Education
12	Defense
13	Aus CERT
14	Internet: Network security and audits

Australia: Australian critical infrastructure includes Communications, Energy, Banking and Finance, Food Supply Emergency Services, Health and Transport and the prime minister has defined the aim of Critical Information Infrastructure Protection (CIIP) as "to assure Australians that both the physical safety of key assets as well as the information technology systems on which so many of them depend are protected" (Abele-Wigert and Dunn, 2006). Key factors of the Australian national security are shown in Table 3.

Canada: Outlining the critical infrastructure is the prerequisite for devolving any security policy. Canada defines its National Critical Infrastructure (NCI) as those "physical and information technology facilities, networks, services and assets, which if disrupted or destroyed would have a serious impact on the health, safety, security or economic well-being of Canadians or the effective functioning of governments in Canada." Government has defined almost ten critical sectors: Energy, Communications and Information Technology, Finance, Health, Food, Water, Transportation, Safety and Manufacturing (Government of Canada, 2004). Table 4 outlines the key factors considered for the Canadian national security.

Table 4: Key factors of the national security (Canada)

Sr. No.	Factors
1	Foreign intelligence
2	Collaboration within government and with international and industry partners
3	Strategic discussion of emergency management issues among key national players
4	Cross-cultural discussion on security issues
5	Legislation
6	Technology and education
7	Defense
8	Economy
9	CanCERT: Canada's first national Computer Emergency Response Team
10	Security certificate

Table 5: Key factors of the national security (China)

Sr. No.	Factors
1	Defense
2	Economic development and security
3	Legitimacy of the Chinese Communist Party (CCP) government
4	Taiwan issue
5	Legislation
6	Skilled diplomacy
7	Geopolitics
8	CNCERT/CC: National Computer Network Emergency Response Technical team/Coordination Center of China Information
9	Security certificate
10	Internal stability

China: The Chinese government has established national security standards relating to infrastructure protection based on international standards such as ISO/IEC and ANSI. China published "Computer Information System Security Protection Classifying Criteria" (GB 17859). GB 17859 defines ten security elements. These ten security elements are integrity, authentication, discretionary access control, object reuse, audit, label, mandatory access control, trusted recovery, trusted path and covert channel analysis (National Criteria of PRC, 1999).

Some examples of national security standards include:

- Encryption technical standards (GB/T 15277, GB/T 17964, GB17901)
- Digital signature standards (GB/T 15852)
- Authentication mechanism (GB/T 15843)
- Physical security and environment protection (GB/T 2887, GB 50174)
- Firewall standards (GB/T 18019, GB/T 18020)
- Proxy server standards (GB/T 17900)
- Router security standards (GB/T 18018)
- Network architecture and security (GB 15278, GB/T 17963)
- Information system security classification standards (GB 17859)
- Security assessment standards (GB/T 18336)

Some of the key factors of the Chinese national security are given in Table 5 (Yang, 2004)

Table 6: Key factors of the national security (European Union)

Sr. No.	Factors
1	European Union wide cooperation
2	Joint responsibility of all stakeholders
3	Public-Private Partnership (PPP)
4	Contingency plans and early warning capabilities
5	Economic and social dimensions
6	Legislation
7	Technology and education
8	Defense
9	CERT: Computer Emergency Response Team
10	European Network and Information Security Agency (ENISA)

European Union: There is a serious concern regarding the national security and national information security in the European countries. The presidency of the council of the European Union elaborate the security issues and its counter measures in the conclusion of the conference held on the hot issue of critical information infrastructure protection (European Union, 2009). According to the literature and author understanding the critical factors which are considered or needs to be considered by the European Union are mentioned in Table 6.

RESULTS

In this study, survey was done for six developed countries for the security factors involved in the development of national security policy. After reviewing the policies of the various countries, it is obvious that the critical infrastructure is a very important step towards the development of the national security policy. However, after defining the critical infrastructure, the focus should be given on the possible threats to those sensitive national organizations and develop the national policy to mitigate those threats and safeguard the national assets.

Moreover, the dominant factors include the political issues for example geopolitics and international cooperation and understanding with other nations of the world; military issues which is focusing on the military alliances of a nation and may also have its roots in national and international intelligence agencies; legislation is an important factor, the presence and the enforcement of laws is a major concern; technical and managerial issues are need to be considered which includes the presence of a team of professionals to deal with any kind of emergency and the security standards which are suppose to be followed in the country, it also has an important aspect of the organizational readiness to adopt the security standards and procedures.

Table 7: Generic factors for the national security

Sr. No.	Factors	Elaboration
1	Political issues	Geopolitics International cooperation Foreign intelligence
2	Military issues	Military alliances Intelligence agencies
3	Legislation	Presence of cyber laws Effective governance Law enforcement
4	Technical and managerial issues	Cyber Emergency Response Team (CERT) Information security standards/security certificates organizational readiness
5	Public Private Partnership (PPP)	The involvement of the private sector in the policy envelopment and implementation is always vita.
6	Research and development	Academic institutions indigenous security products

The last, but not the least, is an important factor of the national security is the research and development; academic institutes can play a vital role. The focus should be given the contemporary security issues and its solution through the novel techniques by involving the promising professionals and the academic institutions. The indigenous development of the security products is also an important aspect of the national security. Some countries like china have their own security standards and products. Table 7 summarizes the discussion and presents key areas of concern and its elaboration for the national security.

DISCUSSION

This study has derived generic dominant factors that should be addressed in the development of national information security policies. The base of the derivation is a wide scope review of policies associated with different nations. From Asia, the policies of Malaysia and China were considered. From south Asia, Australia's policy was taken into account. From North America, the policies of both: the USA and Canada were considered. And from Europe, the policy of the European Union was included. This wide scope view provides confidence in the concluded dominant factors. These factors are less in number than the factors associated with each addressed policy individually, but they conceptually cover all the factors of the addressed policies. They are associated with six main types of issues: "political", "military", "legal", "technical and managerial", "public and Private Partnership (PPP)", in addition to "research and development". The inclusion of all of these issues in a national information security policy will make it well-suited to dealing with practically all national information security problems and that is what makes a policy a good one.

CONCLUSION

In the wide scope review of the national information security policies, given in this study, it has been observed that while many of the factors considered by these policies are of common content, differences also exist leading to some gaps in the various policies. The concluded dominant factors from the various policies help making future policies more comprehensive. Future development of national information security policies, such as the future policy of the Kingdom of Saudi Arabia (KSA), would benefit from considering the dominant factors given in this study.

REFERENCES

Abele-Wigert, I. and M. Dunn, 2006. International CIIP Handbook. Vol. 1, Center for Security Studies, ETH Zurich, pp: 495.

American National Security Policy, (ANSP), 2002. http://ocw.mit.edu/NR/rdonlyres/Political-Science/17-471American-National-Security-PolicyFall2002/

Bruce, R., S. Dynes, H. Brechbuhl, B. Brown and E. Goetz, 2005. International policy framework for protecting critical information infrastructure: A discussion paper outlining key policy issues. TNO Report, Tuck School of Business at DARMOUTH.

European Union, (EU), 2009. Proceeding of the Ministerial Conference on Critical Information Infrastructure Protection, Apr. 27-28, Tallinn, pp: 1-5. http://www.tallinnciip.eu/doc/EU_Presidency_Conclusions_Tallinn_CIIP_Conference.pdf

Federal Information Security Management, (FISMA), 2002. Public Law 107-347 TITLE III-Information Security. http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

Government of Canada, 2004. Government of Canada Position Paper on a National Strategy for Critical Infrastructure Protection. http://www.acpa-ports.net/advocacy/pdfs/nscip_e.pdf

National Criteria of PRC, 1999. Computer information system security protection classifying criteria. (In Chinese). http://www.infosec.org.cn/fanv/03_22.htm

National IT Council, (NITC), 2010. National Cyber-Security Policy (NCSP), Malaysia. http://www.nitc.my/index.cfm?andmenuid=57

Rehman, B.S.A., 2002. Malaysia's approach to network security. Proceeding of the ITU Workshop on Creating Trust in Critical Network Infrastructures, May 7, Malaysian Communications and Multimedia Commission, Malaysia, pp: 1-18. http://www.itu.int/osg/spu/ni/security/workshop/presentations/cni.19.pdf

Ross, R., 2005. Building more secure information systems. Proceeding of the Quarterly IT Forum at GSA Co-Hosted by the IT Workforce Committee of the CIO Council and GSA's Office of Electronic Government and Technology, Apr. 6, National Institute of Standard and Technology. http://www.cioc.gov/Documents/NIST_FISMA_Presentation.ppt

Yan, Q. and H.Y. Shu, 2005. The application of an object-oriented method in information system security evaluation. Lecturer Notes Comput. Sci., 3688: 357-367. DOI: 10.1007/11563228

Yang, J., 2004 China's National Security: Reassessment, Strategy and Policies. University of Auckland. http://www.nziia.auckland.ac.nz