ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Security threats to E-business among SAARC Nations – A Preliminary Study

[1] Rajiv Kumar
Assistant Professor, Punjab Institute of Management & Technology, Mandi Gobindgarh, Punjab, India

Abstract: **- Over the years it has been observed that SAARC nations mainly worked towards development of economic relationship among the SAARC nations. Attempts are also on to further enhance trade relations with the member nations. At the age of the Internet and its evolutionary technologies global business has been envisioned as a big possibility. Despite of various security threats, member nations agreed to formalize manifold activities to boost global business through the use of prevalent internet connectivity. This paper will explore various security issues as trade barrier among neighboring nations, the need to reform the existing cyber laws for promoting international business. Particularly, the paper will highlight necessity of secure cyber framework for boosting e-business among the eight countries of the South Asian Association for Regional Cooperation (SAARC) keeping in mind the three dimensions of security -- confidentiality, integrity and availability..**

Keywords**: Attacks, cyber security, international business, security threats.**

I. INTRODUCTION

South Asia has been experiencing an explosion of awareness, aspirations and identities like many other developing regions. This is the result of shrinking global distances, expanding communication network and technology revolution in almost all the fields that affect human life. Many of the consequences of this triple explosion in this world's most populous region are positive. There is a creative upsurge to find new solutions to prevalent problems. South Asia is a regional group that possesses immense trade potential but the achievement in intra-regional economic integration has been insignificant due to limited regional cooperation. The 18th SAARC Summit held in Kathmandu, Nepal in November 2014, marked the dominion of the "alliance with neighborhood first" principle in the evolving foreign policy of neighboring nations. No concrete action was taken on the issues of terrorism, trade and foreign investment. It was, as always, full of fanfare and rhetoric, and plenty of handshakes and promises were exchanged. On top of the agenda were three connectivity agreements on road, rail and energy. It is well recognized that removal of trade and non-trade barriers would enhance regional cooperation among the SAARC members. The member nations should expedite the connectivity among them even beyond the road, rail connectivity. India's plan to launch a satellite for the South Asian countries in order to expand information sharing and connectivity within the region is globally appraised, although the objective of this satellite is to update weather forecast. Similar efforts will fortify plans and practices to promote cross border business using electronic pathway. Existing cyber laws across various nations are stumbling block in setting up barrier-free communication link leading to underutilization of existing communication link through internet. The eight members of the South Asian Association for Regional Co-operation (SAARC) – Afganistan, Bangladesh, Bhutan, India, Maldives, Nepal, Pakistan and Sri Lanka – are highly underrepresented in the use of the Internet. Representing 22.4 % of the world population, SAARC members accounted for only 0.039 % of the total number of Internet hosts as of July 1999. Economic backwardness, of course, is the major reason for the low level of Internet connectivity in this region. Social, political and cultural barriers, however, are no less important. Internet is the better medium to reach global market in a cost-effective way. Internet can allow emerging nations to leapfrog ahead of their global competitors by skipping several essential stages of technological development. If the enterprises in South Asian countries are unable to employ leapfrogging strategies with regard to Internet, the Information Revolution may prove to be a serious threat rather than an opportunity for them. Various factors like availability, knowledge and trust critically affect the adoption of Internet for commercial transactions to promote global business.

Factors Promoting International Business (Communication and Globalization)

International business organizations must be especially careful in conducting business communication across cultures. It is necessary to try to rise above culturally imbued ways of viewing the world. To do this, one needs to understand how the perception of a given message changes depending on the culturally determined viewpoint of those communicating. With the dawn of globalization, international business is becoming increasingly popular. A

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

company needs to be aware of the language and culture of the country where it plans to embark with its investment. Politics and laws of the nation can either make international business easy or hard. The international business among SAARC nations is not different from this as it is observed from the Table 1 that most prevailing factors communication and globalization are not followed at par. It jeopardizes the possibility of electronic business among SAARC nations.

Communications (2009)								
Items	Afghanistan	Bangladesh	Bhutan	India	Maldives	Nepal	Pakistan	Sri-Lanka
Fixed telephone lines per 100 population	0.4	0.72 (2012)	2.7 (2012)	2.38 (2013)	7 (2012)	3.15(2012)	1.63(2012-13)	13(2013)
Mobile cellular subscriptions per 100 population	39.2	61.5 (2012)	77.4 (2012)	70.63 (2013)	169.5 (2012)	61.8 (2012)	65.64(2012-13)	99(2013)
Internet user per 100 population	3.3	17.7 (2012)	21 (2011)	17.38 (2013)	26.5 (2012)	26.1 (2013)	12	9.8(2013)

Globalization (2010)								
Item	Afghanistan	Bangladesh	Bhutan	India	Maldives	Nepal	Pakistan	Sri-Lanka
Trade in goods balance (% of GDP)	-58.2 (2009)	-6.15 (2012)	-19.50	NA	-69 (2012)	-30.03 (2012)	-6.2 (2013)	-12.9 (2013)
Trade in services balance (% of GDP)	-2.6 (2009)	-2.15 (2012)	-3.30	14.94 (2012)	68 (2012)	0.49 (2012)	-6.4 (2013)	2.0 (2013)
Current account balance (% of GDP)	-3.9 (2009)	1.71 (2012)	-19.17	-4.97 (2012)	-27.1 (2012)	3.71 (2012)	-1.0 (2013)	-3.8 (2013)
Workers' remittances received (USD, million)	NA	12843.4 (2012)	NA	NA	NA	4987.74 (2012)	13920 (2013)	6407 (2013)
Workers' remittances received (% of GDP)	NA	11.06 (2012)	NA	NA	NA	28.29 (2012)	5.9 (2013)	9.5 (2013)
FDI net inflows (USD, million)	185 (2009)	1136.38	NA	2323995.7	164	104.23	1447	540 (2013)

		(2011)		(2012)		(2012)	(2013)	
FDI net inflows (% of GDP)	1.5 (2009)	1.02 (2011)	NA	1.3 (2012)	7.9	0.59 (2012)	0.6 (2013)	0.80(2013)
International reserves (USD, million)	198(2009)	19150.5 (2014)	917 (2012/13)	NA	298 (2012)	955.36 (2012)	11058 (2013)	8574 (2013)
Total external debt (USD, million)	2328(2009)	22095 (2012)	135.56 (2012/13)	NA	962.6 (2010)	3549.72 (2012)	57268 (2013)	39741.2 (2013)
Total external debt (% of GDP)	NA	19.04 (2012)	0.14 (2012/13)	NA	46.4	20.14 (2012)	24.2 (2013)	59.2 (2013)

Table 1: Country-wise share of various items in communication and globalization.

[SAARC in Figures 2014 (Source: http://www.saarcstat.org/content/saarc-figures. Last accessed on 28 Nov 2015)] The significance of regional cooperation organizations, acting as a symbol of growing interdependence and mutual trust, has increased globally to boost cross-nation business. However, in case of SAARC, both the conditions of interdependence and mutual respect have been lacking.

Inter-state Conflicts bloc E-Business among SAARC Nations

The explosion of awareness, aspirations and identities in South Asia has also created new and intensified prevailing social tensions which have taken the forms of agitations and protest movements on the one hand and violent conflicts and organized insurgencies on the other, along religious, political and ethnic lines. While agitations and protest movements are a part of political process and have to be addressed by the governments within the given framework of political and administrative decisions, the insurgencies and violent conflicts threaten to tear the structure of the state apart. The challenge of coping with these conflicts is indeed complex and without meeting this challenge, the stability and development of the State or the region as a whole, cannot be ensured. Thus from the above it is clear that there are two types of conflicts occurs in South Asian region. One is intra-state conflicts and other is inter-state conflict. Intra-state conflicts are these conflicts which occur within the state. Whereas Inter-State conflicts are those conflicts which occurs between the two or more than two states. Intra-state conflicts are the main reasons behind the Inter-state Conflicts and must be dealt with. It is envisioned that for promoting cross-border business the inter-state conflicts of SAARC region must be resolved to harmonize business relations. South Asia is often described as a region full of contentious issues in bilateral Inter-state relations. States located in South Asia have taken longer than expected in overcoming their mutual suspicion and relating to one another as bloc. While India Pakistan relations have often remained troubled, other countries in the region also do not have smooth relations with India – the dominant country within the grouping. India's relation with other SAARC members has been foresighted as troublesome because of existing facts which are out of scope of this paper. Owing to this situation, SAARC has not been able to achieve its potential; although everything in SAARC, by no means, is gloomy. Overall, the prospects in the present setting do not look promising. Involvement of, and increased cooperation with China, ideally full membership, will indeed be beneficial for the whole region. In the long run, the countries of SAARC will also have to find solutions of all outstanding political issues to fully benefit from potential of regional cooperation.

Cyber Security – A Big Global Challenge

While rapid technological developments have provided vast areas of new opportunity and potential sources of efficiency for organisations of all sizes, these new technologies have also brought unprecedented threats like Cybercrime, Cyber warfare and Cyber terror with them. Cybercrime is conducted by individuals working alone, or in organised groups, intent on extracting money, data or causing disruption, cybercrime can take many forms, including the acquisition of credit/debit card data and intellectual property, and impairing the operations of a website or service. A nation state conducting sabotage and espionage against another nation in order to cause disruption or to extract data is declaring Cyber war against that nation. There are proofs of Cyber war in India, Pakistan, Afganistan and Bangladesh. On 4 December 2010, a group calling itself the Pakistan Cyber Army hacked the website of India's top investigating agency, the Central Bureau of Investigation (CBI). The National Informatics Center (NIC) has begun an inquiry (NDTV, 2010). On 26 November

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

2010, a group calling itself the Indian Cyber Army hacked the websites belonging to the Pakistan Army and the others belong to different ministries, including the Ministry of Foreign Affairs, Ministry of Education, Ministry of Finance, Pakistan Computer Bureau, Council of Islamic Ideology, etc. The attack was done as a revenge for the Mumbai terrorist attacks (ETribune, 2011). An organization, working independently of a nation state, conducting terrorist activities through the medium of cyberspace. These are threats of a global nature and we need to develop tools that are different from the ones we had in the past. We need to find ways to help each other to identify common approaches to combating these challenges. Cyber Security is emerging as one of the key areas in international security. Cyber security – defined as the protection of systems, networks and data in cyberspace – is a critical issue for all businesses. Cyber security will only become more important as more devices, 'the internet of things', become connected to the internet. A series of cyber security dialogues have been held in the recent past among SAARC nations. Make in India gives an opportunity to develop ICT as well as cyber security products and services in India. Cyber security will remain a major area of engagement for India with the rest of the world. Leading security agencies are worried about the cyber warfare capabilities of various nations including the main SAARC nations India, Pakistan. Table 2 below illustrates the cyber warfare capabilities of various nations:

	Cyber warfare Doctrine / Strategy		CW training/ Trained Units	CW exercises/ simulations	Collaboration w/ IT Industry and/or Technical Universities
Albania		X	X	X	
Argentina	X		X		
Australia		X	X		
Austria	X		X	X	
Belarus	X		X		
Brazil		X	X	X	
Bulgaria		X		X	
Canada				X	
China	X		X	X	X
Cyprus		X	X	X	X
Czech Republic		X	X	X	
Denmark		X		X	
Estonia		X	X	X	
Finland	X			X	
France	X		X	X	X
Germany	X		X	X	
Ghana		X			
Hungary		X	X	X	X
India	X		X	X	X
Iran			X		X
Israel	X		X	X	X
Italy			X	X	X
Japan			X		
Jordan		X	X		
Kenya			X		
Latvia		X	X	X	
Lithuania		X		X	
Malaysia		X	X		
Netherlands		X	X	X	
New Zealand		X	X		
North Korea			X		X
Norway		X		X	
Pakistan			X		
Philippines		X	X		X
Poland		X		X	
Russia	X		X		X
Slovak Republic		X		X	
South Korea		X			
Spain				X	
Sweden				X	
Switzerland		X		X	
Turkey		X	X	X	
United Kingdom		X	X	X	
USA		X	X	X	

Table 2: Cyber warfare capabilities of Selected Nations

(Source: Survey from Cyber Warfare an Analysis of the Means and Motivations of Selected Nation States (Revised, 2004)) It is evident from the above table that cyber warfare is recently identified as critical key factor to strengthen defending security solutions. Moreover, cyber warfare is an attractive option because no troops are required only one person can create havoc, freely available tools, complete anonymity of attacker, no need to defeat a nation to take control of its public service systems, the effect of cyber war is immediate and give no time to retaliate. Having the right cyber defense and skills is equally important as defense from nuclear disasters. Believing this, various business organizations in SAARC nations are strengthening their defending skills for cyber-attacks. With increase in smartphone users, the business organizations are promoting mobile based business services now though these are more vulnerable to security attacks. Latest security solutions must provide mobile device management along with other security measures to make defensive security system a foolproof.

Possibilities of Cyber Security Frame Work for SAARC Nations

SAARC nations must mandate the development of a foolproof cyber security framework to help nation members in managing cyber security risks. A foolproof information security system has tenets like Confidentiality, Integrity and Availability. Confidentiality is the assurance that information is not disclosed to unauthorized individuals or processes. Information requires protection from unauthorized disclosure. It deals with controlling who gets to read information in computer data and program files or information that may be on hard copy, for example, traditional files, documents etc. Integrity is ensuring that information retains its original level of accuracy. Information must be accurate and complete, and requires protection from unauthorized, unanticipated or unintentional modification. Availability is the timely, reliable access to data and information services to authorized users. Information must be available on a timely basis, wherever it is needed, to meet business requirements or to avoid substantial losses. It deals with assuring that system users have uninterrupted access to information and system resources such as data, programs, and equipment. For such a cost-effective foolproof cyber security framework the collaboration among government sectors and private sector is must. Despite of governance, risk and compliance administrative controls, data and application security, security assurance and monitoring, the cyber security framework must constitute modules capable to anticipate and defend against cyber-attacks, assess organizational readiness to counter such attacks and finally improving existing cyber security posture. The common standards, guidelines and principles critical to global

business should be key concerns of framework. An ideal cyber security framework typically exhibit peculiar characteristics like a) comprehensive and evolving to meet a changing threat profile in order to mitigate the effect of continuously changing security demands of organization in the recent dynamic business environment b) scalability to meet diverse standards prevalent in global business scenario. Crucially, there is no existence of any foolproof cyber security framework in any of SAARC nations.

III. CONCLUSION

In the technological revolution across the globe, there is great risk of vulnerabilities faced by various business organizations. Moreover, the nations can attack each other through cyber battlefield by stealing important strategic information, denial of service attacks on publicly spread infrastructural services, defaming political image of any nation to affect its economy. The identification of dire need for such a secure cyber security framework is well framed in this paper. The critical issues hindering the development and implementation of a common cyber security framework are described and must be addressed through harmonizing relationships, enhancing mutual trust among member nation of SAARC. The collaborative action may bring such a promising cyber security framework to existence in near future.

REFERENCES

1. (Billo, 2004) Billo C & Chang W (2004) “Cyber Warfare an Analysis of The Means and Motivations of Selected Nation States” web link: http://www.ists.dartmouth.edu/docs/execsum.pdf

2. (Deity, 2011) Discussion draft on National Cyber Security Policy “For secure computing environment and adequate trust & confidence in electronic transactions” web link: http://deity.gov.in/hindi/sites/upload_files/dithindi/files/ncsp_060411.pdf

3. (ETribune, 2011) "36 government sites hacked by ‘Indian Cyber Army’". The Express Tribune. Retrieved 8 November 2011

4. (NDTV,2010) "Hacked by 'Pakistan cyber army', CBI website still not restored". Ndtv.com (4 December 2010). Retrieved 8 November 2011.

5. (DSWA, 2015) Donaldson S E, Siegel S G, Williams C K, Aslam A (2015), “Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats” Apress

6. http://www.saarcstat.org/content/saarc-figures. Last accessed on 28 Nov 2015.