SAIS 2009 Proceedings

Southern (SAIS)

3-1-2009

The Impact of Culture on Global Information Security Regulations

Andrew P. Ciganek
Jacksonville State University, aciganek@jsu.edu

Guillermo A. Francia III
Jacksonville State University, gfrancia@jsu.edu

THE IMPACT OF CULTURE ON GLOBAL INFORMATION SECURITY REGULATIONS

Andrew P. Ciganek
Jacksonville State University
aciganek@jsu.edu

Guillermo A Francia, III
Jacksonville State University
gfrancia@jsu.edu

ABSTRACT

The balance between individual privacy and information and security assurance (ISA) regulations is a fluid debate that has many different facets. The objective of this early research is to examine the impact that culture has on ISA regulations. In particular, we examine how internationally accepted ISA policies are adopted in disparate cultures. Multiple interviews were conducted in Thailand with individuals with requisite knowledge on how Internet security was applied in their country. A discussion of these findings is presented, categorized by national culture dimensions and illustrated with examples, followed by some concluding remarks.

Keywords

Information and security assurance, privacy, culture, e-commerce, globalization

INTRODUCTION

The expansion of free trade worldwide accompanied by increasing access to the Internet has ushered in an era of globalized markets. As global commerce increases over the Internet, challenges to individual privacy and security have become as diverse as the number of different countries that participate. Accompanying this increase in diversity is an increasing need for standard information and security assurance (ISA) policies to be adopted to protect data and ensure that global commerce is not hindered. Universal adoption of these ISA policies, however, may be compromised by the diverse cultural values of each nation.

The objective of this research is to examine the impact that culture has on the universal adoption of ISA policies. Consequently, a discussion of the cultural issues influencing legislation and their enforcement are presented examining the state of information security regulation in Thailand. Thailand is uniquely situated on the opposite ends of every national culture dimension with the U.S., and in some instances, the most extreme ends (Hofstede, 2007). For example, the U.S. is characterized as one of the most individualistic cultures (loose bonds with others) while Thailand represents one of the most collectivist cultures (everyone takes responsibility for others). Similar dichotomies exist among both cultures in each of the other national culture dimensions and have been shown to significantly influence differences in perceptions (Ciganek, Jarupathirun and Zo, 2004). Such differences in culture offer opportunities to reveal insights into the various activities that prevail to protect data.

Thailand is an active trading partner of the U.S. and must comply with globally acceptable requirements of Intellectual Property (IP) and privacy protection. This research examines issues in formulating security laws, regulations, and policies that influence the adoption or the non-adoption of internationally recognized standards, such as those advocated by the Asia-Pacific Economic Cooperation (APEC), the EU Directives and Standards, ISO 27002 (also known as Information technology - Security techniques - Code of practice for information security management), and corresponding U.S. regulations. This examination is valuable as these ISA-related laws, regulations, and policies are vital in sustaining a robust, cooperative economic and national security partnership. Further, since the battleground of information warfare has moved to cyberspace, it is paramount for both countries to establish ways and means that will employ a robust and effective cyber infrastructure that will counteract cybercrime and cyber-terrorism. These ISA challenges are not exclusive to a U.S. – Thai partnership. Therefore, this research will have implications for other international trading partners.

In the next section, we will discuss the relevance of ISA policies for global commerce in greater detail. We will also summarize the pertinent national culture dimensions that characterize the U.S. and Thailand. We then discuss the findings from the multiple interviews that were conducted followed by some concluding remarks.

INFORMATION SECURITY AND ASSURANCE (ISA)

The ubiquitous nature of computing infrastructure in our personal, social, and professional lives has raised the importance of ISA issues to a critical level. Such issues include, but are not limited to, the development of rigorous security practices, the means to meet and remain in compliance with federal regulations on information security, the development and deployment of secure applications, the education of an information assurance-aware society, the formation of a secure Internet infrastructure, and the various perceptions of information security and assurance due to cultural differences.

ISA policies refer to the specific activities put in place to protect data (NSA, 2008), of which, there are multiple layers (Laudon and Traver, 2009) (see Figure 1). Multiple layers are necessary to protect data since the best technological solutions (e.g., encryption, firewalls, anti-virus software, etc.) could be subverted without functional organizational policies and procedures in place. Further, industry standards and government laws are necessary both to provide a guideline for the secure transaction of data and to investigate and prosecute those that violate the laws intended to protect data. It is in each of these layers where different cultures likely employ dissimilar approaches to secure data, perhaps to varying levels of success.

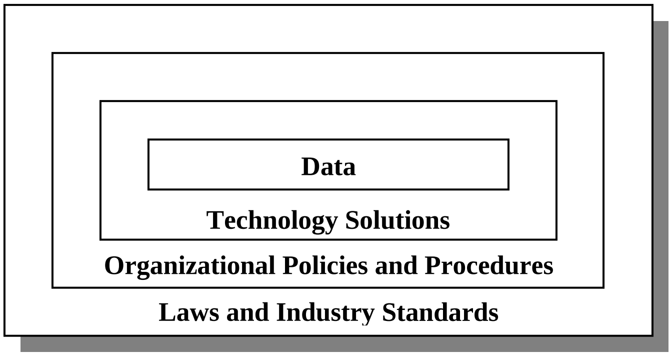
Data
Technology Solutions
Organizational Policies and Procedures
Laws and Industry Standards

Figure 1: Multiple Layers of Activities to Protect Data, Adapted from Laudon and Traver, 2009

A sound security and information assurance program is always built upon strong and sensible policies. These policies, as described in NIST800 (2007), are categorized according to the following three types: enterprise information security, issue-specific security, and system-specific security. The standard practice is to first create the general policy types (enterprise information security) and then create more detailed policies that relate to specific issues and systems (Whitman and Mattord, 2008). Similar to laws and ethics, the development of such policies is greatly influenced by culture and local customs. Consequently, it is imperative that when ISA policies are developed that they be applicable across cultural and ethnic boundaries and that policy makers collaborate, gain competencies with, and are sensitive to foreign cultures. This is consistent with the cyberinfrastructure vision described by the director of the National Science Foundation (Bement, 2007).

Information security and assurance is of vital importance in the United States today as over 245 million data records of U.S. residents have been exposed due to security breaches since January 2005 (PRC, 2008) and the average annual estimated losses due to cybercrime in 2007 were $350,424 per respondent, up from $168,000 in 2006 (Richardson, 2007). Further, the Department of Justice recently released data from its extensive 2005 National Computer Security Survey and reported that a staggering two-thirds of all firms detected at least one cybercrime during that year (Rantala, 2008). To combat cybercrime, there are an increasing set of laws, standards, and regulations[1], which may overlap and be inconsistent, that U.S. organizations struggle to comply with (Francia, Estes, Francia, Nguyen and Scroggins, 2008; Francia and Zanzig, Forthcoming). Further, there are still many industries in the U.S. where such regulations are relatively immature or have yet to be developed, which has had a negative impact on their growth (Ciganek, Haines and Haseman, 2005; Ciganek, Haines and Haseman, 2006). With such immaturity and inconsistencies existing and its impact on the U.S. economy, it is not surprising that there have been numerous calls from research for further insight and learning materials (Bhagyavati, Olan, Naugler and Frank, 2005; Bogolea and Wijekumar, 2004; Katz, 2005; Whitman and Mattord, 2004) as well as government initiatives (DHS, 2003; NIATEC, 2008) that highlight both the national and global importance of ISA.

[1] Federal regulations include the Computer Fraud and Abuse Act (last amended in 2001), Computer Security Act (1987), Health Insurance Portability and Accountability Act (1995); Financial Services Modernization Act (also known as Gramm-Leach-Bliley Act (GLBA), 1999), USA Patriot Act (2001; renewed in 2006), Sarbanes-Oxley Act (SOX, 2002), and the Federal Information Security Management Act (FISMA, 2002).

CULTURAL ISSUES

Culture is theorized to shape the behavior of a collection of individuals (Hofstede and Hofstede, 2004) and has been shown to have a significant impact on decision making processes (Ciganek, Mao and Srite, 2008). Culture is defined as the "interactive aggregate of common characteristics that influence a human group's response to its environment" (Hofstede and Hofstede, 2004: p. 10). Culture establishes social norms and values, which in turn affect individual behaviors and beliefs. There are several different levels of culture that have been examined in the literature (e.g., individual, organizational, national), each with interesting findings. The focus of this research is on culture at the national level since national culture transcends organizational culture in the formulation of laws and regulations. Hofstede and Hofstede (2004) identify five different dimensions of national culture that explain the similarities as well as differences of behavior and belief among individuals in different societies; high/low power distance, individualism/collectivism, masculinity/femininity, high/low uncertainty avoidance, and long-/short-term orientation. Each of these dimensions, with respect to the United States and Thailand, are summarized in Table 1.

Power Distance: Extent less powerful members of organizations accept and expect power distributed unequally	
United States:	**Thailand**:
• Greater equality between societal levels • Cooperative interaction across power levels • More stable cultural environment	• High level of inequality of power and wealth, not necessarily forced upon the population, but accepted by the society as a part of their cultural heritage
Individualism/Collectivism: Degree to which individuals are integrated into groups	
United States:	**Thailand**:
• More individualistic attitude • Relatively loose bonds with others • Self-reliant	• Close, long-term commitment to the member 'group' • Loyalty is paramount • Strong relationships; everyone takes responsibility for others
Masculinity/Femininity: The distribution of roles between the genders	
United States:	**Thailand**:
• High degree of gender differentiation of roles • The male dominates a significant portion of the society and power structure	• Less assertiveness and competitiveness
Uncertainty Avoidance: Tolerance for uncertainty and ambiguity	
United States:	**Thailand**:
• Fewer rules • Does not attempt to control all outcomes and results • Tolerance for a variety of ideas, thoughts, and beliefs	• Strict rules, laws, policies, and regulations are adopted • Goal is to control everything to avoid the unexpected • Does not readily accept change, very risk adverse
Long-/Short-Term Orientation: Concern with virtue regardless of truth	
United States:	**Thailand**:
• Fulfills its obligations • Appreciation for cultural traditions	• Emphasis on thriftiness and perseverance

Table 1: Summary of National Culture Dimensions, Adapted from Hofstede, 2007

Since the United States and Thailand are on the opposite ends of every national culture dimension, and in some instances, the most extreme ends (Hofstede, 2007), we anticipate that there are many insights specific to ISA policies in the U.S. that can be gained by examining how a disparate culture from the U.S. resolves these same challenges. For example, Thailand is characterized as having a low tolerance for uncertainty, which should have an impact on the specific organizational policies and procedures in place. The successes and/or challenges that Thai organizations encounter as a result of their ISA polices, while facing the same security threats as U.S. firms participating in the global economy, should lead to some key insights.

THAILAND'S COMPUTER CRIME ACT (CCA)

The Computer Crime Act (CCA) took effect on July 18, 2007 with the aim of ensuring Internet security and enhancing electronic commerce in Thailand by creating a safer environment that was more conductive to Internet users. A primary goal of the CCA was to eliminate loopholes in existing Thai laws to empower law-enforcement agencies to more effectively deal with cyber crimes like hacking and spamming. As a result, the CCA requires all Internet Service Providers (ISPs) to keep log files of bandwidth consumption, Internet traffic, and records of individual users for 90 days. Without this law, it is argued that law-enforcement officials would be unable to apply the Criminal Code and criminal procedures in order to go after cyber criminals (Nation, 2007). The CCA was based on the ISO/IEC 27001 information security management system standard and also follows the U.S. Department of Defense Directive 8570.1 to ensure that computer forensic examiners are trained and certified to effectively defend information, information systems and information infrastructures. Acceptable certification exams include the Certified Information Systems Security Professional (CISSP), Systems Security Certified Practitioner (SSCP), Certified Information Systems Auditor (CISA), or at least the CompTIA Security+ Certification and Exam. Multiple interviews were conducted in Thailand with individuals with requisite knowledge on how the CCA has been applied. A discussion of the findings in these conversations follows which are categorized by national culture dimensions and illustrated with examples.

Uncertainty Avoidance

Uncertainty avoidance describes the tolerance for uncertainty and ambiguity that is considered acceptable in one country over another. Though the CCA was based on internationally accepted standards, there are a few aspects of its implementation in which Thai culture (high uncertainty avoidance) is reflected. First and foremost, true to its characterization as a culture that is very risk adverse or does not readily accept change, Thailand is several years behind the lead of many other countries in implementing Cybercrime legislation. Interestingly, the origins of the CCA could be traced back to the Internet Promotion Act first forwarded back in 1997 in Thailand and many other policies proposed thereafter. However, all legislation has faced intense opposition by the elected Thai government which has made laws slow to react to the demands and vulnerabilities of today's security environment and has ultimately made such policies out-of-date even before they are ever enacted.

Another feature of the CCA that can be tied to Thai culture is how strict this law is in comparison to Cybercrime legislation implemented elsewhere in the world. Several national and international human rights groups, including Reporters Without Borders and the Asian Human Rights Commission, have criticized Thai legislation like the CCA as both restrictive and repressive. Earlier drafts of the CCA included the death penalty and life imprisonment for computer crimes that cause damage to computers and/or people, but have since been revised to maximum sentences of twenty years and significant fines.

Individualism-Collectivism

The cultural dimension individualism-collectivism refers to the degree that individuals are integrated into groups, which in Thailand is relatively high and collectivist. With respect to a collectivist culture where there are strong relationships that exist and everyone takes responsibility for others, this can be seen directly in some of the language of the CCA. In Thailand, for example, it is possible that individuals or parties be held responsible for cyber crimes even though they did not initiate the crime themselves. Under section 14 of and earlier draft of the CCA, "Any service provider knowing of the perpetrating of an offence under Section 13 [which includes libel, falsifying data, national security breaches, viewing porn or sending porn to friends] within a computer system under their control but failing to delete immediately the computer data contained therein shall be subject to the same penalty as that imposed upon a person committing an offence under Section 13" (FACT, 2007). Consequently, any "service provider", which is language vague enough to include all organizations from Internet Service Providers to local Internet cafés, can face the same fines or penalties (up to five years imprisonment) as if they had committed the cyber crimes themselves (Sambandaraksa, 2008a).

Another feature of a collectivist culture is one in which loyalty is dominant guiding rule in society. This is best illustrated in lèse majesté crimes, or insults against the king of Thailand who is wonderfully revered and respected by all Thai's and is considered a father-like figure, which carry some of the severest penalties for such crimes in the world (RWB, 2008). In other instances where loyalty is paramount, section 20 of the CCA prohibits data from being disseminated which "might be contradictory to the peace and concord or good morals of the people", however, no description is provided of what might cause damage national security or contradict peace and morality (AHRC, 2007). As a result of the lack of any clear direction, this provision could be interpreted to include not only the owners of the content that is perceived as offensive to the country, but those that view that content as well. As stated above, however, what is clear is that a "service provider" can be held liable for any illegal content that is located on their servers.

Although the CCA never refers to censorship because censorship is illegal and unconstitutional in Thailand, there is incentive for service providers to self-censure to ensure that they are compliant. Consequently, it is not uncommon in Thailand for content to be available from one service provide while blocked by another (Sambandaraksa, 2008b). For example, entire access to YouTube was blocked for what was believed to be one unacceptable video (BBC, 2007) while the entire blogging domain Website "Wordpress" was blocked by some ISP's for containing “content, text, and/or picture that is unappropriated which affects the mind of Thai people all over the country and thus cannot be accepted” (Prachatai, 2008c).

Power Distance

Power distance refers to the extent that less powerful members of in a society accept and expect power distributed unequally. This type of behavior is exhibited through the enforcement of the CCA in Thailand in which Thai officials are sometimes viewed as being above the law. Whether such behavior is deliberate or unintentional, it is best described as a “corruption of policy” since it is acceptable practice for Thai officials to describe their potentially illegal action as being in the interest of “national security”. For example, as stated above, censorship is illegal in Thailand, but if a Website is deemed to be offensive to the country or having lèse majesté content, it may be blocked. At times, the “offensive” content that is blocked through the enforcement of the CCA is actually content from opposing political parties or simply opposing political viewpoints (AFP, 2008; Prachatai, 2008a). As another example of a “corruption in policy”, it is believed that since Thai officials can only pursue legal proceedings with Websites registered in Thailand, that a “hack and crack” program is being implemented to hack offensive Websites hosted abroad to delete their contents since the legal process would take too long (Prachatai, 2008b). These examples clearly illustrate the power distance relationships that exist in Thailand.

CONCLUSION

As global commerce increases over the Internet, challenges to individual privacy and security have become as diverse as the number of different countries that participate. The objective of this research is to examine the impact that culture has on the universal adoption of ISA policies. As the initial case from Thailand has shown, there are some stark differences that exist in information security regulations between the United States and Thailand. Consequently, further examination of additional cases in Thailand as well as in other countries would likely lead to additional insights into the impact that culture has on information security policies. A very recent example is the proposed Senate amendment to the Philippines’ Intellectual Property Code that stipulates the adoption of the APEC Privacy Principle, which resembles a closer affinity to local issues and is preventive in nature, rather than the more restrictive EU privacy regulations (Casiraya, 2008). We believe that the successes and/or challenges that organizations from disparate cultures encounter, while facing the same security threats as American firms participating in the global economy, will lead to key insights that can be communicated as best practices to follow. Additional topics that are worthy of academic pursuit include examining the provisions that seem extraordinary in other cultures, the length of time it takes to legislate a law, the factors that influence the depth and breadth of legislative provisions, and the degree of affinity of similar information security legislations in countries that belong to the same region.

REFERENCES

1. AFP (2008) Media Rights Group Condemns Thai Censorship in Name of King Viewed on August 30, 2008, http://news.yahoo.com
2. AHRC (2007) Unintelligible Computer Law Passed Under Junta's Watch, Viewed on July 26, 2008, http://www.ahrchk.net
3. BBC (2007) Thailand Blocks Access to YouTube, Viewed on August 30, 2008, http://news.bbc.co.uk
4. Bement, A.L. (2007) Shaping the Cyberinfrastructure Revolution, Viewed on October 14, 2007, http://www.nsf.gov/news/speeches/bement/07/alb070129_ci_nas.jsp
5. Bhagyavati, Olan, M., Naugler, D., and Frank, C. (2005) Information Assurance in the Undergraduate Curriculum, *Proceedings of the Forty-Third Association for Computing Machinery (ACM) Southeast Regional Conference*, Kennesaw, Georgia, 25-26.
6. Bogolea, B. and Wijekumar, K. (2004) Information Security Curriculum Creation: A Case Study, *Proceedings of the First Annual Conference on Information Security Curriculum Development (InfoSecCD)*, Kennesaw, Georgia 59-65.
7. Casiraya, L. (2008) Senate Must Pass IP, Data Privacy Laws, Viewed on October 7, 2008, http://inquirer.net
8. Ciganek, A.P., Haines, M.N., and Haseman, W.D. (2005) Challenges of Adopting Web Services: Experiences from the Financial Industry, *Proceedings of the Thirty-Eighth Hawaii International Conference on System Sciences (HICSS)*, Big Island, Hawaii, 1-10.

9. Ciganek, A.P., Haines, M.N., and Haseman, W.D. (2006) Horizontal and Vertical Factors Influencing the Adoption of Web Services, *Proceedings of the Thirty-Ninth Hawaii International Conference on System Sciences (HICSS)*, Kauai, Hawaii, 1-10.
10. Ciganek, A.P., Jarupathirun, S., and Zo, H. (2004) The Role of National Culture and Gender on Information Elements in e-Commerce: A Pilot Study on Trust, *Proceedings of the Tenth Americas Conference on Information Systems (AMCIS)*, New York, New York, 470-476.
11. Ciganek, A.P., Mao, E., and Srite, M. (2008) Organizational Culture for Knowledge Management Systems: A Study of Corporate Users, *International Journal of Knowledge Management*, 4, 1, 1-16.
12. DHS (2003) The National Strategy to Secure Cyberspace, Viewed on April 28, 2008, http://www.whitehouse.gov/pcipb/
13. FACT (2007) Draft Cybercrime Bill, Viewed on July 16, 2008, http://facthai.wordpress.com
14. Francia, G., Estes, B., Francia, R., Nguyen, V., and Scroggins, A. (2008) The Design and Implementation of an Automated Security Compliance Toolkit: A Pedagogical Exercise, *Journal of Digital Forensics*, 2, 4, 23-32.
15. Francia, G. and Zanzig, J. (Forthcoming) Security Compliance Auditing: Review and Research Directions, in M.E. Whitman and H.J. Mattord (eds.*)* Readings and Cases in the Management of Information Security.
16. Hofstede, G. (2007) Geert Hofstede Cultural Dimensions, Viewed on October 10, 2007, http://www.geert-hofstede.com/
17. Hofstede, G. and Hofstede, G.-J. (2004) Cultures and Organizations: Software of the Mind, (McGraw-Hill, New York, New York.
18. Katz, F.H. (2005) The Effect of a University Information Security Survey on Instruction Methods in Information Security, *Proceedings of the Second Annual Conference on Information Security Curriculum Development (InfoSecCD)*, Kennesaw, Georgia, 43-48.
19. Laudon, K.C. and Traver, C.G. (2009) E-Commerce: Business, Technology, Society, (Fifth ed.) Prentice Hall, Upper Saddle River, New Jersey.
20. Nation (2007) New Law Takes Aim at Cyber-Criminals, Viewed on July 22, 2008, http://www.nationmultimedia.com
21. NIATEC (2008) Literacy, Awareness, Training and Education: Because There is no Patch for Ignorance, Viewed on September 16, 2008, http://niatec.info
22. NIST (2007) Special Publications (800 Series), Viewed on October 18, 2007, http://csrc.nist.gov/publications/PubsSPs.html
23. NSA (2008) Information Assurance Frequently Asked Questions, Viewed on June 14, 2008, http://www.nsa.gov/ia/iaFAQ.cfm?MenuID=10#1
24. Prachatai (2008a) Exploring 29 Websites Alleged by Democrat Party to Lave Lese Majeste Content, Viewed on July 22, 2008, http://www.prachatai.com
25. Prachatai (2008b) ICT to "Hack & Crack" Foreign Websites Offensive to Thai Supreme Institution, Viewed on August 30, 2008, http://www.prachatai.com
26. Prachatai (2008c) ‘TOT’ blocked Net users from WordPress, Viewed on August 30, 2008, http://facthai.wordpress.com/2007/08/26/tot-blocked-wordpress/
27. PRC (2008) A Chronology of Data Breaches, Viewed on October 1, 2008, http://www.privacyrights.org/
28. Rantala, R.R. (2008) Cybercrime against Businesses, 2005, Viewed on September 28, 2008, http://www.ojp.usdoj.gov/bjs/pub/pdf/cb05.pdf
29. Richardson, R. (2007) Computer Crime and Security Survey, Viewed on October 10, 2007, http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf
30. RWB (2008) Government Steps Up Online Censorship, Viewed on July 26, 2008, http://www.rsf.org
31. Whitman, M.E. and Mattord, H.J. (2004) Designing and Teaching Information Security Curriculum, *Proceedings of the First Annual Conference on Information Security Curriculum Development (InfoSecCD)*, Kennesaw, Georgia, 1-7.
32. Whitman, M.E. and Mattord, H.J. (2008) Management of Information Security, (Second ed.) Thomson Course Technology, Boston, Massachusetts.