CORE
Metadata, citation and similar papers at core.ac.uk
Provided by Research Online @ ECU

Edith Cowan University

Research Online

Australian Information Security Management Conference

Conferences, Symposia and Campus Events

12-4-2013

A Comparison of Information Security Curricula in China and the USA

Huaying Chen
University of Melbourne, huayingc@student.unimelb.edu.au

Sean B. Maynard
University of Melbourne, seanbm@unimelb.edu.au

Atif Ahmad
University of Melbourne, atif@unimelb.edu.au

Follow this and additional works at: https://ro.ecu.edu.au/ism

 Part of the Information Security Commons

Recommended Citation

Chen, H., Maynard, S. B., & Ahmad, A. (2013). A Comparison of Information Security Curricula in China and the USA. DOI: https://doi.org/10.4225/75/57b5629dcd8e1

DOI: 10.4225/75/57b5629dcd8e1
11th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 2nd-4th December, 2013
This Conference Proceeding is posted at Research Online.
https://ro.ecu.edu.au/ism/153

A COMPARISON OF INFORMATION SECURITY CURRICULA IN CHINA AND THE USA

Huaying Chen, Sean B. Maynard, Atif Ahmad
Department of Computing and Information Systems
University of Melbourne, Australia
huayingc@student.unimelb.edu.au, seanbm@unimelb.edu.au, atif@unimelb.edu.au

Abstract
Information Security (InfoSec) education varies in its content, focus and level of technicality across the world. In this paper we investigate the differences between graduate InfoSec programs in top universities in China and in the United States of America (USA). In China, curriculum emphasises Telecommunication, Computer Science and InfoSec Technology, whilst in the USA in addition to Computer Science and InfoSec Technology the curriculum also emphasises Enterprise-level Security Strategy and Policy, InfoSec Management, and Cyber Law. The differences are significant and will have a profound impact on both the perceptions and capabilities of future generations of information security professionals on the one hand, and the management of information security in public and private organizations in the respective countries on the other.

Keywords
InfoSec, Education, Knowledge Protection, China, United States

INTRODUCTION

Rival economic powers, the USA and China recognise the critical role played by information resources in sustaining the long-term economic viability of the modern nation-state. For both countries, the security of these information resources, such as the confidentiality of sensitive information and knowledge, as well as the availability and integrity of information infrastructure must be preserved in the national interest. The responsibility to manage information security falls on future generations of information security specialists that are being educated in tertiary institutions in the respective countries.

An informal review of the literature reveals that although tertiary institutions in both countries have been teaching information security for many years, there is considerable difference in the approach and content. Further, the literature review did not find any studies comparing information security curricula offered in the respective regions.

There are two reasons for undertaking this study. The first is to enable the authors to improve the information security curricula taught at the University of Melbourne. The differences in approach and content can provide insight into the development of information security curricula in Australian Universities. Also, the comparison will enable the authors to better engage with students with prior information security education from China and the USA. The second reason is that research into security curriculum will help organizations gain a deeper understanding of the perceptions, biases and background of information security management staff in the organization.

In this study, China and the USA are regarded as typical representatives of Eastern and Western culture. This research answers the following research question: "*How is InfoSec curriculum different in eastern and western cultures?*" In this paper we adopt the USA terminology for courses and programs. The term "curriculum" in this paper refers to a set of "courses", which refers to the smallest unit for students to have lectures on one topic. Normally, a master's student in Australia has 4 courses per semester which are studied within a "program".

This paper is structured as follows. First we present a discussion of the literature on cross cultural analysis of curricula, in particularly in the information technology domain. We then discuss the research method and the collection of the data. We then present a discussion on the differences of curricula design in China the USA within InfoSec education. Finally we conclude with some recommendations about how these curricula might be amended to cater for the needs of practitioners.

BACKGROUND

We conducted a systematic review of the literature on InfoSec curricula followed by a cross culture analysis. After an exhaustive literature search, relatively few papers were identified that compare InfoSec curricula. Subsequently, as InfoSec can be viewed as a subset of Information Systems (Theoharidou and Gritzalis, 2007), this more general area is investigated.

Information Systems Curricula Comparison

A number of studies have analysed curricula in different countries and show that curricula tended to have greater similarities than differences across nations where they are of like culture (Goslar and Deans, 1994; Cater-Steel et al., 2010; Shen et al. 2008; Hwang et al. 1992). However where differences were found, they were often profound. For instance Cater-Steel et al. (2010) found that the focus of curricula in IT Service Management was technical in Australia, whereas in Canada it was managerial. Studies have also focused on the differences that locale or culture may have on curricula. Hwang et al. (1992) and Shen et al. (2008) found that in China curricula was highly influenced by the Chinese Ministry of Education, and in the USA was highly influenced by the Association for Computing Machinery (ACM). More recently, Li et al. (2010) found that the major difference between USA and Chinese information systems curricula was in its content.

Within these curricula studies a number of variables are used to compare the curricula. These are summarised in Figure 1 and form the basis for our comparison of InfoSec curricula.

InfoSec Curricula Design

Some researchers argue for a top down approach to InfoSec curricula design where they identify the types of jobs a graduate will have and then design the curriculum based on the jobs (Kim and Surendran 2002, Reynolds 2003). Others provide curriculum frameworks and argue for a common body of knowledge (Theoharidou and Gritzalis 2007). Researchers generally argue that InfoSec curriculum should contain aspects of information systems and computer science as well as security fundamentals (Theoharidou and Gritzalis, 2007; Warren and Leitch, 2009). Kim and Surendran (2002) suggest (see Figure 2) that an InfoSec curriculum should cover 18 areas. Furthermore, they suggested that students should initially take the system security course as the foundation of their studies, to be followed by courses on network security and application security.

InfoSec Curricula in China

China has offered InfoSec programs for around ten years. In 2001, WuHan University established the first InfoSec program in China. By the end of 2010, the Ministry of Education granted 64 universities permission to set up InfoSec program (Ministry of the P.R.C., 2012). The Ministry of Education InfoSec Program Higher Education Committee is the prime organisation overseeing InfoSec educational programs. It issues the principles and guides the research for developing and teaching InfoSec Curriculum. Most universities have designed their InfoSec programs based on the committee's principles.

Variables	Definition	Authors
Population	The number of students and faculty	Sa´nchez et al. (2010); Li et al. (2010)
Education History	The period of providing Information Systems education	Hwang et al. (1992); Sa´nchez et al. (2010);
Students Background	The educational level and educational experience of the students	Hwang et al. (1992); Goslar and Deans (1994); Li et al. (2010);
Research and Development Policies	The Policies and regulations supporting or restricting the Information Systems research and development	Sa´nchez et al. (2010);
Education Policies and Standards	The policies and standards supporting or restricting Education	Hwang et al. (1992); Shen et al. (2008); Sa´nchez et al. (2010);
Educational Initiatives and Projects	The number and foci of the ICT/Information Systems educational initiatives and projects	Hwang et al. (1992); Sa´nchez et al. (2010); Cater-Steel et al. (2010);
ProgramSetting	The department which provides the Information Systems	Hwang et al. (1992);
Faculty Background	The educational experience, re-training of the faculty	Hwang et al. (1992); Goslar and Deans (1994); Sa´nchez et al. (2010); Cater-Steel et al. (2010);
Course Contents	An abstract of each course, including course name and the contents covered	Hwang et al. (1992); Goslar and Deans (1994); Xu et al. (2002); Shen et al. (2008); Cater-Steel et al. (2010); Li et al. (2010);
Courses Category	The category of courses, e.g. compulsory, general, professional etc.	Xu et al. (2002); Shen et al. (2008); Li et al. (2010);
Curriculum Architecture	A road map or a structure of the courses consisting the curriculum	Xu et al. (2002); Cater-Steel et al. (2010); Li et al. (2010)
Instructional Materials	The materials used during teaching the courses, including textbooks, cases, journals etc.	Goslar and Deans (1994);
Curriculum Resource Support	The infrastructure of teaching the courses, including hardware and software	Hwang et al. (1992); Goslar and Deans (1994); Sa´nchez et al. (2010);
Teaching Approach	A method to deliver the knowledge to students	Cater-Steel et al. (2010);
Teaching Time	A number of time of having all courses	Xu et al. (2002);
Graduation Requirement	The minimum credits and learning time for graduation	Hwang et al. (1992); Li et al. (2010)
Academic Goal	The expected outcomes after learning the curriculum	Shen et al. (2008); Cater-Steel et al. (2010);

Figure 1 Variables of Information Systems Curricula Comparison

Key Works↓ Education Contents*→	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Analysis of security requirements	●	●											●					
Documentations of security policy	●												●					
Risk analysis	●									●	●	●	●	●	●	●	●	
Selection of safeguards	●	●	●	●	●	●	●	●	●	●	●	●	●	●			●	●
Test of selected safeguard	●		●	●	●	●	●	●	●	●		●	●	●			●	●
Security aggregate planning	●	●												●		●	●	
Safeguard Implementation	●		●	●	●	●	●	●	●	●		●						●
Education and training	●				●	●					●	●	●					
Operation & maintenance		●	●	●	●	●	●	●	●	●		●	●					
Security audit & review	●												●		●			
Emergency response to incidents	●										●		●					
Monitoring			●	●	●	●	●	●	●	●		●	●		●			

* 1: Info security law and standards, 2: Info-system analysis design, 3: System security technology, 4: Database, 5: Operating system, 6: Network security, 7: Intrusion detection and interception, 8: Network, 9: Network security tech., 10: Virus, 11: Hacking case, 12: Web security, 13: E-commerce security, 14: Accounting and finance, 15: Statistics, 16: Risk analysis, 17: Decision theory, 18: Cryptology

Figure 2 Relationships between Contents and the Key Work Functions in InfoSec (Kim and Surendran, 2002)

InfoSec Curricula in the USA

In the USA, InfoSec has traditionally been known as Information Assurance, however more recently programs are being called Information Security or Cyber Security. It has been in development with increasing efforts and enthusiasm for over twenty years (Vaughn, Dampier & Warkentin, 2004; Malladi, El-Gayar & Streff., 2007). 190 institutions in the USA provide programs in InfoSec (NSA, 2012). InfoSec programs in the USA are continuously being assessed and improved, for example: effective approaches to teaching InfoSec and emerging needs for InfoSec curricula are being investigated (Morales and Dark, 2007).

In conclusion, to undertake a curricula comparison in different nations, a conceptual framework should be established firstly to guide the comparison. Subsequently, the 17 factors identified in Figure 1 will be used as a lens in this study.

RESEARCH METHOD

The purpose of this research is to compare the InfoSec curricula from China and the USA. As these curricula were documented in textual form, this research uses document analysis as its main research method (Cater-Steel et al., 2010; Sánchez, Salinas, & Harris, 2010). Following this method, the InfoSec Curriculum characteristics were firstly studied focusing on the one country, and then considering corresponding variables of both countries.

Universities' documentation, research papers and publications from professional organisations, as well as government departments are the basic data sources of this study. Since the objects of this study are the InfoSec Curricula offered by universities in China and the USA, the curricula documentation are the main data source of the research, including syllabuses, training plans, course reports etc. Furthermore, even though a comparative study on InfoSec Curriculum is not available so far, some researchers have analysed the situation of InfoSec program in their countries (Kim and Surendran, 2002; Zhang et al. 2008; Warren and Leitch, 2009). This information provides guidance and evidence for this research. Moreover, some government departments and professional organisations have also issued important standards and proposed recommendations for InfoSec curriculum development.

In this study we selected 10 universities from each country. These universities had to offer an InfoSec program (as defined by the Ministry of Education of the P.R.C. 2012; & NSA 2012) and the top 10 ranked universities with such a program were used from each country (based on ranking lists by RenMin University 2011 and the U.S. News 2011). The selected Universities are shown in Figure 3.

China	U.S.
Peking University（1）	Johns Hopkins University （13）
Fudan University（3）	Georgetown University (21)
University of Science and Technology of China（7）	Carnegie Mellon University (23)
Shanghai Jiaotong University（8）	University of Southern California (24)
Nankai University（10）	University of California--Davis (38)
WuHan University （14）	Pennsylvania State University--University Park (46)
Tongji University（19）	University of Illinois--Urbana-Champaign (46)
Beijing University of Science and Technology（28）	University of Washington (46)
Beijing University of Posts and Telecommunications （42）	Boston University (51)
University of Electronic Science and Technology of China（45）	The George Washington University (51)

Figure 3 Selected Universities (numbers in brackets show rankings)

RESULTS

This section presents the results of the curriculum comparison based on the 17 factors identified in Figure 1 which have been grouped into 8 areas:

1. InfoSec Program Profiles (*Population, History, Students Background*)
2. Policies and Standards (*Research and Development, Education, Initiatives*)
3. *InfoSec Program Setting*
4. *Faculty Background*
5. Curriculum (*Course Contents, Course Category, Curriculum Architecture*)
6. Instruction (*Instructional Material, Curriculum Resources, Teaching Approach*)
7. Graduation Requirements (*Teaching Time, Requirements*)
8. *Academic Goal*

InfoSec Program Profiles

Information regarding the history, population and student background for InfoSec programs in each country is presented in Figure 4. InfoSec programs in the USA are more mature and more widely spread throughout universities (3% vs 9%). This indicates a much larger scale of offering InfoSec Curriculum in the USA than in China, especially when the relative populations of each country are considered. On average there are about double the number of students in Chinese Universities undertaking security study, and subsequently more staff are involved. Both countries require students with high levels of academic background at both the undergraduate and postgraduate level (top 10%~20%).

Information Security Program		China	U.S.
History	Year Information Security Program Started	2001	Late 1980s
	Number of Uni. Offering Information Security Curriculum	64	190
Population	Average Number of Information Security Students (approximate)	60 (UG)	30 (UG)
		30(PG)	15 (PG)
	Average Number of Information Security Faculty (approximate)	20	15
Students Background	Undergraduate	Top 20% (NCEE)	Top 20% (GPA, SAT); Teacher Evaluations
	Graduate	Bachelor Degree; Top 20% (NPEE)	Bachelor Degree (Better in Science or Engineering), Top 10% (GPA, GRE), Recommendation Letters

Figure 4: InfoSec Program History, Population and Student Background

Policies and Standards

Information on the Policies and Standards applicable in each country are shown in Figure 5. These policies and standards affect the curriculum provided within each country's InfoSec programs and affect the way in which students are taught about InfoSec.

Policies and Standards	China	U.S.
Research and Development Policies	N/A	N/A
Education Policies and Standards	N/A	NSTISS, proposed by InfoSec Institute (INFOSEC)
Education Recommendations	Several, proposed by the Ministry of Education Information Security Program Higher Education Committee	Several, Proposed by professional organisations, such as ACM, IEEE, etc.

Figure 5: A Comparison of InfoSec Policies and Standards

Even though many government regulations, federal laws and standards about InfoSec were promulgated in both China and the USA. These focus on crime, government department responsibilities and individual responsibilities. Policies and standards focusing on InfoSec research and development from an educational perspective were non-existent. However, in terms of education standards, the USA published a National Training Standard for Information Systems Security (NSTISS), while there was no such education standard in China. InfoSec curriculum development was guided differently in each country. In China, recommendations were provided by the government (Ministry of Education InfoSec Program Higher Education Committee), whilst in the USA they were provided by professional organisations (ACM, IEEE etc.).

InfoSec Program Setting and Faculty Background

The location of the InfoSec program within each of the Universities shows that there are differences between China and the USA (Figure 6). In China, there was a tendency to place the InfoSec program in a Computer Science or Telecommunication Engineering department. However the trend in the USA was to place the program in less technical areas (information systems and InfoSec departments).

	Security Program Location		Faculty Background	
Domain	China (10)	U.S. (10)	China	U.S.
Telecommunication Engineering	4	0	37.1%	1.7%
Engineering	0	1	0.0%	0.0%
Computer Science	4	2	31.3%	35.3%
Information Systems / Information Science	1	3	4.1%	23.1%
Information Security / Information Assurance	1	4	6.8%	25.9%
Mathematics	0	0	19.7%	3.5%
Others (Business, Law, Health Science etc.)	0	0	0.0%	10.5%

Figure 6: Location of InfoSec Programs and Staff Background

Figure 6 also shows that the background of the faculty teaching into the programs is also skewed in a similar way. Across both countries the majority of faculty had PhD qualifications (more than 95%), however in the USA these tended to be less technical qualifications than faculty from China. Faculty in the USA covered a wider range of knowledge and skills and thus could offer a wider range of topics in the InfoSec programs.

Curriculum

As the main component of this study, the curriculum reflected the principal character of an InfoSec program. The data (Figure 7) shows that whilst curricula differ between Universities within each country, the content tended to be fairly similar. However, when looking at each country there is a large difference between the programs offered. InfoSec courses could be classified within 3 domains:

Telecommunication, Computer Science, and InfoSec. Even though Telecommunication courses seemed irrelevant to InfoSec, Chinese educators regarded them as fundamental InfoSec Curriculum, whereas no University in the USA offered these courses. Courses on InfoSec Management, Security Policy, and Cyber Crime were widely provided by USA universities but were rare in China.

Courses Offered	Core	Elective	China (10)	Core	Elective	U.S. (10)
Analog Electronic Technology	7		7			0
Basic Circuit Theory	6		6			0
Telecommunication Fundamentals	9		9			0
Digital Electronic Technology	8		8			0
Signals and Systems	7		7			0
Digital Signal Processing	6		6			0
Digital System Design	7		7			0
Compiler Principles	8		8			0
Computer System and Interface Technique	5		5			0
Information Theory and Coding	7		7			0
Principles and Applications of Embedded System	7		7		3	3
Computer Network	10		10	5	1	6
Software Engineering	8		8	3	1	4
Operating Systems	10		10	9		9
Computer Organisation Architecture	10		10	5		5
Database Management	10		10	8	2	10
Data Structure and Algorithms	10		10		5	5
Object Oriented Programming	10		10	8		8
Mathematic Fundamentals of Information Security	10		10			0
Introduction to Information Security	10		10	10		10
Cryptography	10		10		8	8
Network Security	10		10	10		10
Electromagnetism Protection and Physical Security		5	5			0
Steganography		9	9			0
Computer Virus and Defence		10	10		7	7
Internet security protocols and related analysis		5	5		5	5
Operating Systems Security		7	7		7	7
Network Content Security		9	9		4	4
Information System Security Evaluation		5	5		6	6
Software Security		7	7		7	7
Security Laboratory		10	10		10	10
Data Recovery		8	8			0
Digital Forensics		3	3		10	10
Designing Security Systems		1	1		6	6
Information Security Management		2	2		10	10
Information Security Risk Analysis		1	1		10	10
Healthcare Security Management			0		3	3
Information Security Policy			0		7	7
Ethics in Security			0		6	6
Enterprise Security and Privacy			0		5	5
Financial Issues in Managing a Secure Operation			0		3	3
Information Security Consulting			0		5	5
Information Warfare			0		3	3
Global Cybercrime Law			0		8	8
Computer Crime		1	1		7	7

Figure 7: A Comparison of the InfoSec Courses

In terms of the core courses, the situation in China and the USA indicated a significant divergence. In most Chinese universities, knowledge on telecommunication and computer science was regarded as the basis of InfoSec and was thus core to programs. To a certain extent computer science was also regarded as important by some USA educators, and subsequently courses such as Database Management, and Programing are core in some programs. Overall, the technical vs Managerial nature of courses is skewed towards the USA with courses in areas such as policy, ethics and consulting only being offered in USA Universities.

Instruction

The manner in which instruction takes place differs for instructional materials and curriculum resources, but is similar for teaching approaches in both countries (Figure 8). In China there is a much higher reliance on text books for instruction (93.2% vs 76.7%) and in the USA more focus was placed on academic papers. Furthermore, in China, where a text was used, over 68% of the programs used one of three texts; sourced from Beijing University of Posts and Telecommunications (BUPT), Tsinghua University (THU) or the educational division of Ministry of Information Industry (MoII). In contrast, educators in USA universities chose textbooks from a wider range, including other universities (32.9%) and other researchers in industry or institutes (35.4%).

Instructional Materials		China	U.S.
Textbooks	From In-house	17.10%	8.40%
	From Other Universities or Educational Department	BUPT 20.3% THU 25.2% MoII 23.1%	32.9.%
	From Other Researchers	7.70%	35.40%
Non-textbook		6.80%	23.30%

Figure 8: Instructional Materials

Even though the InfoSec teachers in China and the USA held differing views in choosing textbooks, they shared the same teaching approaches (Figure 9). Approximately 50% of the teaching is lecture based and the remaining time is practical.

Teaching Approaches	China	U.S.
Lecture-based	53.70%	50.10%
Workshop or Laboratory	30.10%	29.50%
Design Project	16.20%	20.40%

Figure 9: Teaching Approach Ratios

Graduation Requirements

The result of the survey on graduation requirements illustrated distinct requirements for InfoSec programs in China and the USA (Figure 10). Students in the USA spend more hours on InfoSec courses than in China, although in China the requirement of a final security project (6 months undergraduate, 1.5 years postgraduate) meant that there was less in-class time. The required mark (percentage) to achieve the minimum standard in courses was different in each country (China: 60%, USA: 50%), but this mark in both countries indicated an average performance level.

Requirements	China	U.S.
Average Minimum Number of Hours for Courses	2452 (UG)	2739 (UG)
	877(PG)	1574 (PG)
Minimum GPA	60/100 (60%)	2.0/4.0 (50%)
Final Project in Security	Required (UG)	Not Required (UG)
	Required (PG)	5/10 Required (PG)

Figure 10: Graduation Requirements

Academic Goal

Each Country's InfoSec programs specified different goals for education. In China, the focus was on the telecommunication, computer science and InfoSec fields whereas in the USA it was on understanding InfoSec theory and technology, as well as business applications of InfoSec.

To determine whether the curricula from both countries are useful in practice, we can look at InfoSec education from two perspectives: the requirements of job roles (Figure 11), and widely-recognised standards (Figure 12). In Figure 11, ten essential skills identified from a survey of 50 InfoSec-related jobs posted on job seeking websites (Monster China/U.S., 2012) are presented. These essential skills illustrate that most InfoSec jobs required candidates to have an understanding of both technology and management, independent of the job location. From the comparison of the skills taught in InfoSec programs in both countries it is evident that USA programs offer a more comprehensive set of skills that are valuable to employers. Additionally for jobs advertised in China they are unlikely to be able to find Chinese graduates to fill some positions based on their academic backgrounds.

Essential Skills	Required in Chinese Industry	Covered in Chinese Universities	Required in the U.S. Industry	Covered in the U.S. Universities
Enterprise-wide Information Security Risk Assessment and Mitigation	100%	1	100%	10
Enterprise Security Policies Development	82%	0	96%	7
Security Events and Incidents Detection and Response (Network and Systems)	100%	8	100%	10
Web Application Vulnerability Scanning and Resolving	88%	10	90%	8
Security System Proposal Development	96%	1	88%	6
Security Log Management and Monitoring	100%	10	98%	10
Servers and Systems Operations and Maintenance	100%	10	100%	10
Antivirus Analysis and Prevention	96%	10	90%	7
Enterprise Encryption Standards Development and Support	80%	10	78%	8
Access Control	84%	0	80%	6

Figure 11: Job Skills: Match Between Skills Required and Taught

ISO/IEC 27000, the most widely-recognised world standard for security, suggests how organisations should manage security (ISO/IEC 27000, 2009). From these suggestions, the knowledge requirements to apply the standards can be identified (Figure 12). Universities in the USA covered more of the knowledge required for ISO/IEC 27000 implementation than Chinese universities. However, no InfoSec program from either country covers all of the areas identified in the standards.

Contents of ISO/IEC 27002	Covered in Chinese Universities	Covered in the U.S. Universities
Risk Assessment and Treatment	1	10
Security Policy	0	7
Asset Management	3	6
Human Resources Security	0	0
Physical and Environmental Security	5	0
Communications and Operations Management	9	8
Access Control	0	6
Information Systems acquisition, Development and Maintenance	1	6
Information Security Incident Management	8	10
Business Continuity Management	0	8
Compliance (policies and standards, and technology)	0	3

Figure 12: Coverage of ISO 27000 Series Knowledge

DISCUSSION

The results of the InfoSec curricula comparison demonstrated more differences than similarities in the curricula offered in the selected universities in China and the USA (Figure 13).

Some of the differences between the USA and China can be explained by the maturity of InfoSec education in the USA As Universities have had about 10 years more experience with InfoSec in the USA it follows that the market penetration is more widespread with more Universities offering InfoSec education. Furthermore, the depth and breadth of knowledge taught by these security programs has been born from experience. USA programs offer students more choices of InfoSec electives within their courses and these tend to have a managerial focus when compared to the prescribed courses in Chinese Universities.

Given the courses that are being taught in USA programs it follows that staffing should be appropriately skewed towards the managerial aspects of InfoSec and this is born out through the analysed data. However with InfoSec programs in both countries having about 1/3 of staff with a Computer Science background, the reliance on Computer Science courses used to provide a fundamental background to InfoSec programs is not surprising.

Perhaps one of the most overriding drivers of differences between InfoSec programmes in China and the USA is that the influence of the government in China is more pronounced, with the Ministry of Education specifying curriculum causing programs to contain many core courses, especially from technical areas. Subsequently students are limited in their elective choices. Chinese InfoSec programs are regarded as an interdisciplinary and applied science of technology on Mathematics (Cryptography), Telecommunication, and Computer Science (Shen et al., 2007). Whereas in the USA InfoSec is viewed as an interdisciplinary and applied science of Computer Science, Informatics, Management (Dark, Ekstrom, and Lunt, 2006; Hentea & Dhillon, 2006). This in turn dictates somewhat where InfoSec programs are located in the University structure.

Area	Similarities	Differences
Information Security Program Profiles	Both countries required the students taking Information Security with a higher academic performance.	Information Security curricula had been offered longer with a larger scale in the United States than China.
Policies and Standards	Policies and Standards focusing on Information Security research and development were non-existent	A recognised education standard was established in the United States, while no such a standard had been published in China. In China the Government guided curriculum, whereas in the U.S. it is guided by professional
Information Security Program Setting	None	Most Chinese universities offered Information Security curricula in Telecommunication or Computer Science Departments. In the U.S. it is in Information Systems or
Faculty Background	Nearly 1/3 faculty had their PhD in the domain of Computer Science in both China and the United States.	The faculty teaching Information Security programs had academic backgrounds in Telecommunication Engineering, Computer Science, and Mathematics in China, compared to Computer Science, Information Systems and Information Security in the United States.
Curriculum	Information Security curricula in both countries required computer science courses as a foundation for Information Security	Universities In the U.S. offered a wider range of courses within an Information Security Program. Information Security curricula in China emphasised a solid foundation on Telecommunication, which was totally opposite in the United States. Students in U.S. universities had more freedom to arrange their courses wheras in China most curses were
Instruction	Similar teaching approaches were used in both countries.	U.S. universities focused on a wider variety of text books and academic papers than their Chinese counterparts.
Graduation Requirements	Both universities in China and the United States required graduates to have an average level of academic performance.	Projects were required at both the Undergraduate and Postgraduate level in china for all courses, but only at the postgraduate level (in 5 universities) in the U.S.
Academic Goal	None	Chinese Information Security curricula focused on leaning the technology, while curricula in the United States focused on supporting business with Information Security

Figure 13: A Summary of Similarities and Differences

CONCLUSION

Although industry in both China and the USA demand that information security professionals have knowledge and skills in enterprise information security management (ISM), such as risk, policy, and incident response (see Figure 11), students who have studied information security in China are not likely to have been educated in these areas. Further, students from China are more likely to have a narrow (technical) information security education whereas their American counterparts are likely to have a broader education and more varied experiences depending on the expertise of their former teaching staff.

Given the authors teach a graduate-level "course" on information security management with a large number of international students from both Western and Eastern countries, the implication is that unlike students from the USA, students from China may not understand how organizations identify, assess and control security risks, how policies are developed and implemented, and how incident response teams identify, contain and eradicate threats.

Organizations intending to employ information security professionals are not likely to find graduates with the requisite knowledge and skills in China. This has implications for Chinese firms in particular because it implies they are better off hiring from Western countries like the USA. An interesting new area of research may be to investigate the information security practices of organizations where management is from China as opposed to the USA. Further, multinationals rolling out information security practices

across subsidiaries in China and the USA may need to consider the respective backgrounds of information security specialists in their implementation program.

On the basis of the research findings and the investigation of industry needs we make three recommendations regarding InfoSec curriculum:

1. Provide less emphasis on Telecommunication courses in China. The current Chinese InfoSec Curriculum contains many Telecommunication courses that are not required by InfoSec-related jobs and are also not relevant to the ISO/IEC 27000 series standards. A thorough knowledge of Telecommunication is not required in InfoSec programs.
2. Include InfoSec Management courses in Chinese InfoSec programs. Many InfoSec related jobs require knowledge on InfoSec Management. Furthermore, the ISO/IEC 27000 standards emphasise the significant position of InfoSec Management. However, Chinese InfoSec programs lack managerial InfoSec courses.
3. Provide courses on Knowledge Protection in both countries. The ISO/IEC 27002 standard recommends organisations to practice Human Resource security, which focuses on protecting knowledge leakage from employees' activities. Additionally, ISO/IEC 27000 defines "Information" as "data and knowledge", which indicates that protecting knowledge is an important component of InfoSec. Therefore, Knowledge Protection courses should be included in the InfoSec Curriculum.

This research can be extended within investigating more universities in the sample, and to look at other Eastern and Western countries. Furthermore, the study would be more comprehensive including the similarities and differences in terms of InfoSec Industry, Information Educational Initiatives and Projects, Education Finance, Curriculum Resource, and Socio-culture in China and the USA.

REFERENCES

Cater-Steel, A., Hine, M. J., & Grant, G. (2010). Embedding IT service management in the academic curriculum: a cross-national comparison. *Journal of Global Information Technology Management*, 13(4), 64-92.

Dark, M., Ekstrom, J., & Lunt, B. (2006). Integrating Information Assurance and Security into IT Education: A Look at the Model Curriculum and Emerging Practice. *Journal of Information Technology Education*: Research, 5(1), 389-403.

Goslar, M. D. & Deans, P. C. (1994). A Comparative Study of Information Systems Curriculum in US and Foreign Universities. *Data Base* 25(1), 7-20.

Hentea, M., Dhillon, H. S., & Dhillon, M. (2006). Towards changes in information security education. *Journal of Information Technology Education*, 5, 221-233.

Hwang, B., Whinston, A., & Savenye, W. (1992). Management information systems curricula in the United States and the Republic of China', *SIGCSE: Technical Symposium on Computer Science Education*, 113

ISO/IEC 27000:2009, (2009). Information technology — Security techniques — Information Security management systems — Overview and vocabulary, International Organization for Standardization, Geneva, Switzerland, Available at: http://standards.iso.org/ittf/licence.html

Kim, K. Y., & Surendran, K. (2002). Information security management curriculum design: A joint industry and academic effort. *Journal of Information Systems Education*, 13(3), 227-236.

Li D., Paranto, S, & Rong, Y. (2010). Management Information Systems curricula: a comparison between China and the USA, *Research In Higher Education Journal*, 6, pp. 1-19

Malladi, S., El-Gayar, O., & Streff, K. (2007, June). Experiences and lessons learned in the design and implementation of an Information Assurance curriculum. *Information Assurance and Security Workshop*, 2007. IAW'07. IEEE SMC (pp. 22-29).

Ministry of Education of the P.R.C., (2012). Ministry of Education of the P.R.C. website, Beijing, viewed 15th Oct. 2012, < http://www.moe.gov.cn/>

Monster China/US, (2012). Monster Jobs Website, Viewed 15th Oct. 2012, < http://www.monster.com/geo/siteselection>

Morales, L., & Dark, M. (2007). Information Security Education and Foundational Research. *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on System Sciences*, 269-269 (January).

NSA (2012). National Security National Information Assurance Education and Training Program (NIETP), National Security Agency, Fort Meade, viewed 15th Oct. 2012, <http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml >

RenMin University (2011), RenMin University of China, Beijing, viewed 15th Oct. 2012, < http://edu.people.com.cn/GB/14894813.html >

Reynolds, C. W. (2003). An undergraduate information assurance curriculum. *Information Assurance Workshop*, 2003. *IEEE Systems, Man and Cybernetics Society*, 10-16, June.

Sánchez, J, Salinas, Á, & Harris, J (2011). Education with ICT in South Korea and Chile, *International Journal Of Educational Development*, 31(2), 126-148

Shen, C., Zhang, H., Feng, D., Cao, Z., & Huang, J. (2007). Survey of information security. *Science in China Series F: Information Sciences*, 50(3), 273-298.

Shen, G., Liu, B., & Zhu, J. (2008). Research on Comparison of MIS Curriculums between China and USA. *4th International Conference on Wireless Communications, Networking and Mobile Computing, 2008. WiCOM'08.* 1-5, October.

Theoharidou, M., & Gritzalis, D. (2007). Common body of knowledge for information security. *Security & Privacy, IEEE*, 5(2), 64-67.

U.S. News, (2011). *U.S.News & World Report* LP. U.S. viewed 15th Oct. 2012, < http://colleges.usnews.rankingsandreviews.com/best-colleges/rankings/national-universities/data >

Vaughn, R. B., Dampier, D. A., & Warkentin, M. B. (2004). Building an information security education program. *Proceedings of the 1st annual conference on Information security curriculum development,* 41-45, October.

Warren, M & Leitch, S, (2009). Information Security management curriculum development: an Australian example, *INSITE 2009 : Proceedings of the 2009 Informing Science + Information Technology Education Conference*, Informing Science Institute, Macon, Georgia, 25-33

Xu, Y., Xu, Z., & Zhang, J. (2002). A comparison of nursing education curriculum in China and the United States. *Journal of Nursing Education*, 41(7), 310-316.

Zhang, A. Xue, Z. Li, J. Meng, K. Lu, S. (2008). Curriculum System of Information Security Engineering for Undergraduates, *Research and exploration in laboratory*, Vol. 28, No.3, pp. 62-64