ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 8(21), DOI:10.17485/ijst/2015/v8i21/79119 September 2015* ISSN (Online) : 0974-5645

Analysis of the Competencies of Information Security Consultants: Comparison between Required Level and Retention Level

Se-Yun Kim[1], Seong Taek Park[1] and Mi Hyun Ko[2*]

[1]Department of Management Information Systems, Chungbuk National University, Korea; ktadslpro@nate.com, solpherd@cbnu.ac.kr
[2]Department of Policy Research, Korea Institute of Science and Technology Information, Korea; mihyungo@kisti.re.kr

Abstract

Recently, the increasing demand of information security consulting and securing workforce for information security consulting companies have emerged as major pending issues especially with the expansion information and communication infrastructures and the increase of instances of personal information leakage. This research aims to provide guidelines for successful information security consulting and training of information security consultants by looking into the core competencies of information security consultants and how much one possesses each competence. Thirty-five competency models were constructed by exploring previous researches, interviewing the experts in the field of information security consulting, and surveying information security consultants on the required and retention level of each competence. The results of the present research can provide useful information in improving the quality of information security consulting services by understanding the differences between required and retention level of competencies among information security consultants.

Keywords: Competencies, Information Security Consultant, Information Security Consulting, Required Level, Retention Level

1. Introduction

Due to the Advanced Persistent Threat (APT) and the frequent cyber-attacks targeting the press and financial institutions, there is a need for critical infrastructures that even the government has announced for the designation of major information and communication infrastructures. Similarly, the demand for information security consulting is expected to greatly increase due to the expansion of major information and communication infrastructures and consulting with the agency in possession, including the financial world, is predicted to sharply increase as well due to card information leakage situation[1]. As the demand of security consulting increases, the government added more information security consulting companies in March of 2014 from 7 to 18 companies in 10 years to improve the information security services and to solve manpower shortages. However, the manpower shortage in the security consulting market stillremains unsolved because the supply cannot meet the growing demand of consulting. Subsequently, consulting companies are expecting competition to intensify due to the information security consulting demand and the expanding size of consulting companies and procurement at a low cost would increase[2]. The intensification in management of consulting companies brings about turnovers among security consultants. The demand for information security consultants is great but analysis on their competencies for manpower training, education and development are lacking. Thus, this research illustrated a competency model through an inquiry into the existing business knowledge and skills of information security manpower

* *Author for correspondence*

and experts. For the empirical analysis, a survey on the required and retention levels of the competencies was conducted among information security consultants.

2. Theoretical Background

2.1 Overview of Information Security Consulting

The information security consulting refers to independent consultation services (dictionary of IT terms, Telecommunication Technology Association) that analyzes the risks that may occur in all Information Technology (IT) assets (e.g. computer system and networks) and organizations. It establishes measures and further supports the administrator and the organization in realizing the said measures. Furthermore, it is defined as a series of processes starting from the establishment of security provisions, assessment of threats, simulation hacking, establishment of master plan, etc. to the security of information and communication infrastructures and systems (Notification on designation of knowledge information security consulting companies, Ministry of Science, ICT and Future Planning notification no. 2013-176). The notification on pre-inspection of information security is defined as consulting accomplished with analysis and assessment of the vulnerability of information system and with a proposal for protective measures based on the assessment and the construction of Information Security Management System (ISMS), as its main purposes in preparation of electronic infringement.

Information security consulting requires a consulting environment appropriate for the company and organization. It is diversified into fragmentary consulting, creating various services such as the construction of Information Security Management System, the establishment of personal information management system and the analysis and assessment of the vulnerability of major information and communication infrastructures.

2.2 Overview of Information Security Consultant

An information security consultant is an expert in analyzing the level, vulnerability and core resources of the information security system of an organization and in suggesting the optimum resolution based on the demand level of the customers[3]. Furthermore, an information security consultant establishes the information security policy, controls over the approach and operation of the system and protects the information asset by promptly detecting and responding to intruders. The information security consultant is the defender or preventer against unauthorized persons who illegally access the information resource of the computer system and perform offensive actions such as taking, falsifying and destroying information[4]. The role of information security consultants is to review the organization's information security policy, standard and procedure and more. This is summarized as follows:

- Review of information security policy of the client organization.
- Assess the standard monitoring processes and procedures of an organization's information security system.
- Investigate each member's responsibilities and roles related to information security.
- Identify the weak points of the current network of the organization and then introduce solutions.
- Plan the structure of the overall security system of the organization to protect its core information.
- Recommend to the management to regularly revise the information security environment of the organization.
- Train the managers and administrators of the client organization regarding the trends and products of information security.

3. Related Researches

3.1 Knowledge for Information Security Professionals

Researches on information security have focused on differentiating the knowledge and skills necessary for the educational process of information and communication as a part of the field of information and communication[5]. Knowledge means the logical judgment system acquirable through learning or practicing whereas technical skills are the experiences, methods, means, efforts, etc. needed in actually carrying out the knowledge[6].

Logan[7] proposed a security management system by connecting knowledge and skills related to information security, security construction and model, operating system security, etc. with the educational process among university students. Cockcroft[8] proposed the knowledge and skills related to internet security for online transactions including access control system and methodology, network security, cryptology, etc. and the

Table 1. Knowledge and Technology required for Information Security Area by Scholar

Scholar	Related knowledge and technology
Cockcroft[8]	Commercial internet security, security standard and protocol, code law, authorization, PKI(Public Key Infrastructure), firewall, data integrity, intrusion verification and inspection, information war, mobile e-commerce security, wireless application security, risk management/disaster restoration, e-money/SET(Secure Electronic Transaction)/SSL(Secure Sockets Layer), Cookies, access control system and methodology, telecommunication and network security, application and system development security, security architecture and model, operation security, business continuity plan, law/survey/ethics, physical security, security strategy, communication skills, technology standard, company standard, government standard.
Logan[7]	Security management work, security architecture and model, access control system and methodology, application development security, operation security, physical security, code law, telecommunication/network/internet security, business continuity plan, law/ survey report/ethics, inspection and monitoring, vicious code, distributed processing security, electronic commerce security, server structure, intrusion detection, response plan, etc.
Irvine et al.[9]	Application ability of math/science/engineering knowledge, data analysis and interpretation/experiment design and performance ability, system/constituting factor/procedure design ability to meet desirable requirements, cooperating ability of team of multiple professional fields, verification/establishment/solution ability for designed problem, understanding of occupational/ethical responsibility, effective communication ability, comprehensive education necessary to understand the influence of designed solution, recognition of necessity for lifelong education, knowledge on current issues such as cyber laws, ability to use technology/corporations/latest devices, well-rounded social relationship and leadership, analysis and understanding of new security environment, system goal, pre-and-post relationship of system, experiential inference ability, knowledge consolidation ability, verification ability of related inferences, verification ability on inferences and results, conclusion induction ability.
Myung-Gil Choi et al.[11]	DB security technology, e-Biz security technology, related laws and regulations, establishment of measures for managerial information protection, basic cryptology, network security protocol, design of physical security measures, backup technology, security inspection, design and management of security module, analysis of security environment, control of computer viruses, design and application of security API(Application Program Interface), smart card security, code protocol design, code mathematics, code application ability, risk analysis and assessment, mobile communication security technology, management of authentication certificate, management of information protection education programs, assessment of information protection system, analysis on vulnerability of information protection system, establishment of information protection policy, information protection consulting, information protection standard, understanding of information warfare, detection of intruder and blocking management, management of and design of key, communication security technology, privacy and ethics, response to hacking.
Hyo-Jung Jeon et al.[5]	Personal privacy and ethics, ability to establish managerial information protection policy, understanding and application ability of basic cryptology, network and communication security technology, database security technology, physical security, ability to design physical information protection measures, ability to analyze security vulnerability, security inspection, analysis and understanding of new security environment, biometrics, ability to establish server security system, new information protection technology, creation and analysis technology of malicious codes, application security technology, risk management (risk analysis and assessment) ability, e-commerce security technology, laws and regulations on information protection, information protection standard, ability to analyze information protection vulnerability, assessment and authorization of information protection system, occupational ethics and professionalism, intrusion detection and blocking management ability, response ability against intrusion accident, contents security technology, digital forensics, ability to analyze and respond to hacking and viruses, COBIT(Control Objectives for Information and related Technology), cyber law, information security management system (ISMS), IT Infrastructure Library (ITIL), PC security technology.

discussed result here is related to the college curriculum. Irvine et al.[9] claimed that the knowledge and skills related to computer security and are necessary for the system design or implementers should be included in the education process of computer science or engineering, proposing a total of 11 knowledge and skills[9].

After analyzing 33 wanted ads for CISO posted in Chief Security Officer Magazine, Whitten[10] suggested knowledge and technology required for a CISO (Chief Information Security Officer). A CISO is required to possess knowledge such as insight on IT security policies, management capability, IT security education, ability to manage relationship with vendors, disaster restoration plan and ability to analyze security vulnerability and technology such as IT security, communication, system operation career, leadership and research and analysis ability.

Choi et al.[11] revealed the knowledge and technical skills necessary among information security experts through the Delhi method and a survey, classifying the researcher group and workers group. As a result, the knowledge and skills proposed by the study have amounted to a total of 15, including the establishment of information security, assessment of information system, analysis of the vulnerability of information security system, program management of information security education, etc. Jun et al.[5] defined the information security manpower and investigated and analyzed the awareness on the degree of requirement and degree of skill by 4 occupations[5]. The result has shown that the knowledge and skill on the field of information security that showed significant differences totaled to 5 which include the understanding of the data base security skill, ability to construct server security system, ability to design and develop information system, proficiency in the technology of PC security, etc.

3.2 Competence of Information Security Consultants

Aside from the knowledge on the information security, an information security consultant has a fundamental competence necessary for the consulting work. In a research by Cho[12] and Jang et al.[13], the 4 most important fundamental competencies in order to become a true information choice are effective communication ability, problem-solving capability, writing logically and presentation. Some other fundamental attitudes in being an information security consultant are the following:

Objectively observe and analyze the present status of the customer's information security system and recommend an appropriate solution based on his/her thorough experience as an information security expert.

The differentiated value deliverable through the consulting services should be judged and the procedure from the discovery of business to the contract should be subdivided and managed.

Information security problems should be seen from the perspective of a manager and optimum solution appropriate to the situation of the customer should be suggested based on facts and analyses. The consultant should consistently support the customer for an effective solution.

After initiating a consulting project, a constant communication with the customer regarding the progress method of consulting and training method, etc.

4. Research Design and Methods

For an empirical analysis of the differences between the constructions of competency model, required level and retention level of information security consultant, the following procedure is accomplished.

According to earlier researches on the required skills and knowledge, manpower and the work accomplishment competency of information security consultants are examined in the 1st stage. Moreover, the competency model comprised of 28 items exploring knowledge and skills, managing the information security of Korean National Competency Standards (NCS), demands of recruitment of information security consultants, work guidebook for security consultants of the Small and Medium Business Administration, etc.

In the 2nd stage, the final competency model is constructed by conducting a pilot test regarding the information security consultant capability model constructed at the preceding stage, which involved 5 information security consultants.

In the 3rd stage, a survey was conducted which lasted from November 9 to November 20, 2014, involving information security consultants. The survey was given to information security consultants through email, online distribution or personal visit. A total of 66 surveys were collected. Among the collected surveys, only 60 were considered as usable data identified through hallo effect, omission of data, etc. SPSS 18.0 and Excel were used for the analysis of the collected data.

Table 2. Competencies of Information Security Consultants (35 Competencies)

Competency
Understanding the project target client company
Understanding the project process method and tool
Project management
Knowledge and experience of management
Method of realizing statistics and analysis result on current situation
Understanding of program sources and programming ability
Understanding of network, system, security and IT services application
Understanding of IT on physical security
Grasping present condition of network, server, and application system and ability to diagnose
Learning and understanding of the technology manual on computation equipment and facilities
Understanding of the basic operation of network, server, and application system
Understanding IT trends related to information security
Grasping and analyzing present condition of information system asset/risks
Understanding of laws and regulations on information security
Designing and establishing information security master plan
Understanding of standards and criteria related to information security
Analyzing vulnerability of information system
Evaluating and accrediting information system
Grasping the scenario on anticipated threats
Grasping industry trends related to information security
Establishing and grasping definition, range, and relation between targets of information security
Establishing of plan for diagnosis and improvement of personal information security
Customer service
Basic foreign language
Leadership
Thinking skills
Understanding and creating documents
Teamwork
Presentation
Human network
Sincerity and responsibility
Exerting efforts in developing relationships with domestic and foreign persons concerned
Appearance and attire
Self-development
Privacy and morals

5. Data Analysis

5.1 Required Level of Competence of Information Security Consultants

After ranking the required competency level of information security consultants, understanding of laws and regulation related to information security was ranked the highest (4.37), followed by grasping and analyzing the current condition of information system assets and risks (4.18) and establishing and grasping definition, range and relation between targets of information security and understanding and writing documents (4.17). Items which were rated relatively low were basic foreign language (2.67), understanding of program sources and programming ability (2.9) and knowledge and experience of management (3.15).

Korea has laws concerning information security such as the 'Protection of Communication Secrets Act', 'Act on the Protection of Information and Communication Infrastructure', 'Law regarding the promotion of information and communication network use and security of information', 'Law regarding the security of personal information of public institution', 'Law regarding the protection and use of location information', etc. The information security consultant should provide or inspect issues and recommend actions based on his/her experiences related to information security for the effective implementation of the laws on information security. Moreover, the actual work of consulting starts when the project is obtained by receiving the Request for Proposal (RFP) from the customer and then submitting the proposal after the review. Since the submission marks the end of the report, the weights of writing the documents and presentation are high.

5.2 Retention Competency Level of Information Security Consultants

The analysis of results on retention competency level of information security consultants were observed. The retention level of sincerity and responsibility was shown to be the highest. This indicates that information security consultants have the sense of responsibility to thoroughly complete the given tasks and emphasize their clear professionalism even though they belong to the work group with high employee turnover rate.

Confidentiality is one of the fundamental principles among people who provide these services. The

consultants should not make personal profits by revealing the confidential data of a customer or providing it to other consulting company or other customers. Due to the nature of the work, the awareness of privacy and morals ranked high.

5.3 Differences between the Required Level and Retention Level of Competency of Information Security Consultants

In showing differences between the required level and retention level of competency of information security

Table 3. Differences between the Required Level and Retention Level of Competency of Information Security Consultants

Competency	Required Level (a)	Retention Level (b)	Differences (a-b)
Leadership	4.03	3.08	0.95
Understanding the project target client company	4.10	3.17	0.93
Understanding of laws and regulations on information security	4.37	3.43	0.93
Project management	4.05	3.15	0.90
Analyzing vulnerability of information system	3.92	3.08	0.83
Thinking skills	4.13	3.32	0.82
Establishing of plan for diagnosis and improvement of personal information security	4.03	3.25	0.78
Presentation	4.10	3.32	0.78
Establishing and grasping definition, range, and relation between targets of information security	4.17	3.42	0.75
Grasping and analyzing present condition of information system asset/risks	4.18	3.45	0.73
Understanding of standards and criteria related to information security	4.02	3.30	0.72
Evaluating and accrediting information system	3.58	2.87	0.72
Understanding of network, system, security and IT services application	4.12	3.40	0.72
Grasping present condition of network, server, and application system and ability to diagnose	4.12	3.42	0.70
Human network	3.82	3.13	0.68
Understanding and creating documents	4.17	3.50	0.67
Designing and establishing information security master plan	3.93	3.27	0.67
Understanding IT trends related to information security	3.85	3.20	0.65
Exerting efforts in developing relationships with domestic and foreign persons concerned	3.85	3.23	0.62
Customer service	4.00	3.40	0.60
Teamwork	4.13	3.55	0.58
Self-development	3.87	3.37	0.50
Understanding the project process method and tool	3.90	3.43	0.47
Grasping the scenario on anticipated threats	3.82	3.35	0.47
Understanding of the basic operation of network, server, and application system	3.73	3.28	0.45
Grasping industry trends related to information security	3.53	3.13	0.40
Understanding of IT on physical security	3.60	3.23	0.37
Privacy and morals	3.97	3.60	0.37
Learning and understanding of the technology manual on computation equipment and facilities	3.52	3.20	0.32
Sincerity and responsibility	4.12	3.80	0.32
Method of realizing statistics and analysis result on current situation	3.75	3.45	0.30
Knowledge and experience of management	3.15	2.90	0.25
Understanding of program sources and programming ability	2.98	2.75	0.23
Appearance and attire	3.52	3.50	0.02
Basic foreign language	2.67	2.67	

consultants, leadership was ranked the highest (0.95). It was followed by understanding of project target client companies and understanding of laws and regulations related to information security (0.93) and project management (0.90). On the other hand, basic foreign language was the lowest (0.00), followed by appearance and attires (0.02) and understanding of program sources and programming ability (0.23).

6. Conclusion

This research defined the concept of information security consulting and information security consultants and constructed a competency model for information security consulting which is composed of 35 items after reviewing previous researches and interviewing experts in the field. A survey on the required level and retention level by competency was conducted among information security consultants. The result has shown that for the required level, the understanding of laws and rules on information security, grasping and analyzing the current condition of information system asset/risks, establishing and grasping definition, range and relation between targets of information security and understanding and writing documents are high while basic foreign language, understanding of program sources and programming ability, knowledge and experience of management activities are low. For retention level, sincerity and responsibility was the highest, together with privacy and morals and teamwork. Relatively, the low items are basic foreign language, understanding of program sources and programming ability, evaluating and accrediting information system. For the difference between the required level and retention level, leadership was shown to be the highest whereas basic foreign language was ranked the lowest.

Therefore, based on these results, direction for education and career development of information security consultants can be suggested as follows; first, it is necessary to focus education on leadership which shows greatest difference between required level and retained level because leadership as well as driving force is essential to effectively achieve the goals of an organization or a project. Next, in order to understand customer company for the project, knowledge should be acquired on organizational culture and business strategy and the level of capability must be enhanced to manage projects through schedule and risk management. Rather than education for basic foreign language and programming ability with relatively smaller difference in level, education to improve ability in laws and regulations related to information protection and in analysis on the vulnerability of information system is considered even more necessary. The result of the present study is expected to be utilized in providing information to program developments for consultant education and career development for existing or new manpower in an information security service company. A limitation of this research would be the failure to secure enough samples due to the evasion by liaisons and avoidance by survey respondents.

In the future, the competency of information security consultants will be evaluated through a new competitive alternative if a competency-based personnel management, classified into groups of hands-on workers and administrators, is introduced alongside a bilateral assessment of level. Moreover, we expect to identify the competency affecting the quality of information security consulting or customer satisfaction after studying consultants and the staff of client companies who participated in information security consulting projects.

7. References

1. Spill and Certification issues, Security Consulting market. Boan News. 2015 Feb 25. Available from: www.boannews.com.
2. Information security consulting market. Digital Times. Available from: http://www.dt.co.kr. 2015.02.25.
3. Worknet. 2015 Feb 25. Available from: http://www.work.go.kr.
4. Lee YD. Creative in the age of Digital. 2015 Mar 25. KRIVET. Available from: http://www.krivet.re.kr.
5. Jun HJ, Yu HW, Kim TS. Analysis on knowledge and skills for information security professionals. Information Systems Review. 2008; 10(2):253–67.
6. Kim YK, Choi WS. A study on the taxonomy for knowledge/skill about information security for information education & practical utilization. Business Education. 2009; 23(3):123–40.
7. Logan PY. Crafting an undergraduate information security emphasis with in information technology. Journal of Information Systems Education. 2002; 13(3):177–82.
8. Cockcroft S. Securing the commercial Internet: Lessons learned in developing a postgraduate course in information security management. Journal of Information Systems Education. 2002; 13(3):205–10.
9. Irvine CE, SK Chin,Frincke D. Integrating security into the curriculum. Computer. 1998 Dec; 31(12):25–30.

10. Whitten D. The chief information security officer:an analysis of the skills required for success. Journal of Computer Information Systems. 2008 Mar; 48(3):15–9.
11. Choi MG, Kim SH. Analysis of knowledge and skill for security professionals. Asia Pacific Journal of Information Systems. 2004 Dec; 14(4):71–85.
12. Cho MH. Consulting foundation. NewJean. Korea. 2006.
13. Jang SS, Jo TH, Shin SH, Shin DC. Establishing and applying of the information security management system. Life & Power Press. Korea. 2013.