

# Comparison of Security Education Program of Woman Information Security Majors of Seoul Region

Jin-Keun Hong

Professor, Division of Information Communication Technology, Baekseok University

## 서울지역 여성 정보보호전공의 보안교육 프로그램 비교

홍진근

백석대학교 ICT학부 교수

**Abstract** With the development of IT technology, along with the expansion of women's participation in society, the education training of information security women's workforce is becoming a very important issue. Therefore, it is important to analyze the relevant curriculum to identify the direction of fostering women's information security workforce. Therefore, in this paper, the education and training programs of the department for training women's information security workforce based in Seoul area of the Korean metropolitan area were analyzed. The main research objective of this paper is to review whether the education and training system, which consists of the department of women's information security human resources development, is in line with the direction of NIST's human resources development. The research focus was on what the women's information security department organizes courses with each security major and what task training is interested in. In addition, in this paper, we were confirmed that the curriculum of the relevant major is based on the NIST Human Resources Development Framework, and that the majors of the relevant universities have an education and training system that conforms to the relevant task. In conclusion, the related majors are judged to be focused on the development of certification evaluation personnel of convergence industry security or information security development personnel, and general cyber security personnel.

**Key Words** : Security, Education, Workforce, Competency, Security major

**요약** IT기술의 발전에 따라, 여성인력의 사회 참여 확대와 함께 정보보호 여성의 인력 양성은 매우 중요한 이슈가 되고 있다. 그러므로 여성 정보보호 인력 양성의 방향을 파악하기 위해 관련 교육과정을 분석하는 것이 중요하다. 따라서 본 논문에서는 국내 수도권의 서울 지역에 소재하고 있는 여성 정보보호 인력 양성 학과의 교육훈련 프로그램을 분석하였다. 본 논문의 주된 연구 목표는 여성 정보보안 인력양성 학과가 구성하고 있는 교육훈련 체계가 NIST 인력양성 방향과 부합하고 있는지 검토하는 것이다. 연구 초점은 여성 정보보안 학과가 보안 전공별로 어떤 특성을 가진 교육과정을 편성하는지, 그리고 어떤 직무 교육에 관심을 가지는지에 초점을 맞추어 연구하였다. 또한 본 논문에서는 해당 전공의 교육과정이 NIST 인력양성 프레임워크를 기준하여, 관련 대학의 전공들이 해당 직무에 부합하는 교육훈련 체계를 가지고 있음을 확인할 수 있었다. 결론적으로 말해, 관련 전공들은 융합산업 보안의 인증 평가 인력이나 정보보안 개발인력, 그리고 일반적인 사이버 보안 인력 양성에 초점을 맞추고 있는 것으로 판단된다.

**주제어** : 보안, 교육, 인력, 역량, 보안 전공

\*This project is sponsored of project funding of Baekseok University.

\*Corresponding Author : Jin-Keun Hong(jkhong@bu.ac.kr)

Received September 2, 2020

Accepted October 20, 2020

Revised October 8, 2020

Published October 28, 2020

## 1. Introduction

Countries around the world are eager to study artificial intelligence technology, a key technology in the Fourth Industrial Revolution. Artificial intelligence technology is the technology that will become the food of the future. But from a security perspective, it can be used to identify security vulnerabilities, while it can also be used to attack attackers. Many female workers in the information security area prefer software development or software development security. Of course, there is a high interest in software development based on artificial intelligence technology.

With the development of IT technology, along with the expansion of women's participation in society, the education training of information security women's workforce is becoming a very important issue. However, there has been no previous research on what standards women's information security personnel are being educated to train. Thus, in this paper, we found the need for comparative research on NIST cybersecurity task standards, which are the criteria of the cybersecurity framework workforce training framework, and the human resources training program of the department that trains female information security personnel.

In this paper, the Department of Information Security for Women in Seoul area of Korea studied with interest what kind of security education courses it is running. This interest begins with the perception that other security development areas or maintenance areas are equally important, as well as the importance of software development security, including artificial intelligence, in the security job favored by women's information security majors. Because the department of women's information security majors organizes the curriculum based on the demand and interest of female students in that major.

Therefore, in this paper, we describe the technology of security related to security tasks presented in the standard NICE standard cybersecurity education curriculum. The NICE program is the National Institute of Standards and Technology (NIST) standard cybersecurity education curriculum and is a good guide line to use when establishing a national information protection curriculum [1-7].

First, we would like to review the relevant research on cybersecurity education in this paper. D. Yuan reviewed the design and implementation of cybersecurity curricula and security training [8]. A. Lodgher and others presented improved models in cybersecurity education [9], and also focused on cybersecurity education [10].

S. Azadegan and M. Olearly reviewed the digital forensics curriculum [11], while Shiva Azadegan and others introduced NSA's Cyber Operations Training Program [12]. K. Kim and others analyzed around the cybersecurity ecosystem and raised the need for various studies on the area of cybersecurity [13].

N. Miloslavskaya and A. Tolstoy focused on educational relevance to cybersecurity frameworks [14], while Conklin Arthur and others were interested in NICE findings [15].

I. Alsmadi and M. Zarour was interested in cybersecurity training in Middle Eastern countries [16]. B. D. Caulkins and others were interested in security management and research, including the National Cybersecurity Manpower Framework [17].

So far, related research has focused on cybersecurity education programs that are practically necessary. However, there was no approach in terms of information security education specialized for female information security majors.

Therefore, in this paper, we intend to analyze the curriculum by linking it between NICE standard guidelines and programs for fostering

women's information security personnel, and to present the appropriate curriculum required in the future.

This paper analyzed the security education course conducted for women's information security majors based in Seoul and tried to diagnose the direction of fostering women's information protection personnel.

Our attention was relatively less on what criteria the relevant majors organized when they launched the cybersecurity training program and how well the program was suitable for the job.

Our interest is to examine the training course of the corresponding major in training female information protection personnel, and to determine which of the information protection tasks the female personnel is suitable for.

The composition of this paper is as follows. First, Chapter 2 describes NICE's security duties and related technical capabilities. Chapter 3 describes the security education course for women's information protection majors located in Seoul. And analyze the curriculum by major. And we conclude in Chapter 4.

## 2. Key security technologies for cyber security task

This technology includes risk management, information assurance, system testing and evaluation, legal ethics, personal safety and security, information system and network security, vulnerability assessment, computer network defense, password, security, cryptography, crime law, computer forensics, public safety and security, accident management, forensics, information system security certification, communication security management in according to NIST standard.

## 3. Comparison of Security Education Program

### 3.1 SungShin Women's University(Dept. of Convergency Industrial Security Engineering)

In this section, as shown in Table 1, the security-related curriculum of Sungshin Women's University's Department of Convergence Industry Security Engineering was analyzed.

**Table 1. Curriculum(Shungshin Women) vs. NIST security technologies**

Key security technologies	opened security subjects (Sungshin Women)
Risk management	•Trend of risk & crisis management
Information assurance	
Information system and network security	•Network security practices •OS&system security practices •Web security practices •DB security practices
Computer network defense	•Information system architecture
Communication security management	
Security	•Introduction of convergency industrial security •Introduction of information security •Introduction of information security management system •Digital security lecture •Convergence security special lecture
Cryptography	•Crypto application&practices
Crime law investigation	•Convergency industrial security investigation procedure theory
Legal ethics	•Understanding of Law & standard of information security
Computer forensics	•Forensics method & introduction theory of evidence
Forensics	•Digital forensics practices
Public safety and security	•Privacy & Internet ethics
Personal safety and security	•Private security & business utilization theory
Vulnerability assessment	•Hacking program practices •Malicious code analysis practices •Hacking program practices2
Accident management	
Information system security certification	•Business information security management system practices •Privacy management system practices •Information security product evaluation method theory •Information security consulting techniques •Information security product security evaluation methodology

Looking at the security curriculum of Sungshin Women's University's Department of Convergence Security Engineering, common training contents on computer network defense, communication security management, and accident response management in terms of information guarantee or security control are missing. Instead, the university's major focuses on the area of convergence industry security, as the department's name suggests. Therefore, we specialize in security education related to convergence industry security. It is strengthening education on the management system process for corporate information or personal information or the security assessment standard design or evaluation method for information security products. The university's curriculum is understood to focus on fostering women's information protection personnel in charge of tasks such as ISMS, CC evaluation, and consulting in the area of convergence industry security.

### 3.2 Seoul Women's University(Dept. of Information Security)

In this section, as shown in Table 2, the security-related curriculum being opened by the Department of Information Security at Seoul Women's University was analyzed.

**Table 2. Curriculum(Seoul Women) vs. NIST security technologies**

Key security technologies	opened security subject (Seoul Women)
Risk management	
Information assurance	
Information system and network security	<ul style="list-style-type: none"> <li>•Windows Security and operations practices</li> <li>•Network security and programming practices</li> <li>•Software security</li> <li>•System security and operational practices</li> <li>•Web application security</li> <li>•Artificial intelligence and information security</li> </ul>
Computer network defense	<ul style="list-style-type: none"> <li>•Intrusion detection and Firewall System</li> </ul>

Communication security management	<ul style="list-style-type: none"> <li>•Mobile security</li> </ul>
Security	<ul style="list-style-type: none"> <li>•Introduction of computer and information security</li> <li>•Current trends in information security industry technology</li> </ul>
Cryptography	<ul style="list-style-type: none"> <li>•The basics of the modern cryptography application</li> <li>•Modern cryptographic application and practices</li> </ul>
Crime law investigation	
Legal ethics	
Computer forensics	<ul style="list-style-type: none"> <li>•Digital forensics</li> </ul>
Forensics	
Public safety and security	
Personal safety and security	
Vulnerability assessment	<ul style="list-style-type: none"> <li>•Windows security malicious code foundation</li> <li>•Malicious code</li> </ul>
Accident management	<ul style="list-style-type: none"> <li>•Cyber terrorism and information warfare</li> </ul>
Information system security certification	<ul style="list-style-type: none"> <li>•Information security software development capability certification</li> <li>•Information security management system certification</li> </ul>

The Department of Information Security at Seoul Women's University runs a general curriculum on information security. However, it does not include courses specialized in risk management or information assurance, courses on public and private safety and security, and education related to criminal investigations and legal ethics. The department's curriculum emphasizes education on security, such as OS systems and networks, and web and AI. It also emphasizes the subject of information system security certification.

### 3.3 Ewha Womans's University(Cyber Security Major)

In this section, as shown in Table 3, the security-related curriculum being opened by the Cyber Security Major at Ewha Womans's University was analyzed.

**Table 3. Curriculum(Ewha Womans) vs. NIST security technologies**

Key security technologies	opened security subject (Ewha Women)
Risk management	•Risk management and intrusion detection system
Information assurance	
Information system and network security	•Information system security •Cyber physical system security •Blockchain application •Web security and practices •Big data security •Network security •Cloud computing security
Computer network defense	•Risk management and Intrusion detection system •Security control
Communication security management	•Information security management •Mobile security
Security	•Introduction of cybersecurity •Cybersecurity foundation project •Secure coding and practical project •Biometric security •Cybersecurity integration project •Information security technology •Cybersecurity industry academic practical design •Cybersecurity short-term internship •Cybersecurity Intermediate intership •Cybersecurity self-design learning •Cybersecurity global field training
Cryptography	•Modern Cryptographic foundation •Information security protocol
Crime law investigation	•Cyber legal policy
Legal ethics	
Computer forensics	•Digital forensics
Forensics	
Public safety and security	
Personal safety and security	
Vulnerability assessment	•Malicious code and practice project •Cyber terrorism and information warfare
Accident management	
Information system security certification	

Ewha Womans University's Cybersecurity major emphasizes education on the latest technology in security. However, education on

information guarantee, public and private safety and security, and accident response management and information system security certification are not included. The direction of education at the university emphasizes general information security technology and cybersecurity education. And it reflects the latest technologies such as big data security and block chain.

### 3.4 Duksung Women's University(Cyber Security Major)

In this section, as shown in Table 4, the security-related curriculum being opened by the Cyber Security Major at Duksung Women's University was analyzed.

**Table 4. Curriculum(Duksung Women) vs. NIST security technologies**

Key security technologies	opened security subject (Duksung Women)
Risk management	
Information assurance	
Information system and network security	•Blockchain •Python hacking programming •Network security programming
Computer network defense	•Internet of things security •Intelligence security project
Communication security management	
Security	•Introduction of Cybersecurity
Cryptography	•Basic cryptography •Applied cryptography
Crime law investigation	
Legal ethics	
Computer forensics	•Digital forensics
Forensics	
Public safety and security	
Personal safety and security	
Vulnerability assessment	•Simulated hacking •Malicious code
Accident management	
Information system security certification	

The curriculum of Duksung Women's University's Cybersecurity major has been excluded from the common required information

security curriculum, such as risk management, information guarantee, communication security management, public and private safety and security, accident response management, and information system security certification. On the other hand, there are courses such as Blockchain, Python, and IoT security, which are the latest technologies. The curriculum of Duksung Women's University's Cybersecurity major has been excluded from the common required information security curriculum, such as risk management, information guarantee, communication security management, public and private safety and security, accident response management, and information system security certification. They are subjects such as Blockchain, Python, and IoT security. The curriculum of Sungshin Women's University's Department of Convergence Security focuses on fostering human resources for system certification evaluation related to the convergence industry sector. However, areas of information assurance, security management and accident response management need to be supplemented. According to an analysis of the curriculum of the Department of Information Protection at Seoul Women's University, the curriculum seems to be faithful to the basic framework of information security. The curriculum of this department does not include subjects of crime and law investigation or ethics, public/private safety and security. According to an analysis of the curriculum of Ewha Womans University's Cyber Security Corporation, the curriculum focuses on security technology and cybersecurity, which reflect new technology trends. This major's curriculum includes information guarantee, public/private safety and security, accident response management and information system security certification. What is unique is the cyber security major, which lacks the curriculum for accident response management.

As a result of analyzing the curriculum of the Cyber Security Corporation of Duksung Women's University, the curriculum includes the basic education of cyber security and the basic curriculum of information security. The curriculum for this major does not include courses on risk management, information guarantee, telecommunication security management, law investigation and ethics, public and personal safety and security, accident response management, and information system security certification. Likewise, there is no subject for accident response management even though it is a Cyber Security Agency.

#### 4. Conclusion

In this paper, the curriculum of the department of information security for Women located in Seoul area was analyzed. As a result of analyzing the curriculum, we can identify the goal and direction of training of human resources for each major. The analysis criteria were based on the common curriculum presented by NICE and compared with the curriculum of the university.

Based on the standards of NIST cybersecurity job technology, this paper analyzes the characteristics of the curriculum in the department of women's information protection in Seoul, Korea. Until then, there was no such approach. And the advantage of this research is to identify the direction of training information protection personnel and the characteristics of information protection job skills promoted by women's information protection human resources training departments in Seoul.

#### REFERENCES

- [1] C. Curricula. (2017). *Curriculum guidelines for*

- post-secondary degree programs in cybersecurity.*  
New York : IEEE Computer Society.  
[https://cybered.hosting.acm.org/wp/wp-content/uploads/2018/02/csec2017\\_web.pdf](https://cybered.hosting.acm.org/wp/wp-content/uploads/2018/02/csec2017_web.pdf)
- [2] W. Park & S. Ahn. (2017). Enhancing Education Curriculum of cybersecurity Based on NICE. *KIPS Trans. on Comp. and Comm. Sys.*, 6(1), 321-328.  
DOI : 10.3745/KTCCS.2017.6.7.321
- [3] S. Hong. (2018). A Study on the Framework of Comparing New Cybersecurity Workforce Development Policy Based on the ATE Programs of U.S. *Journal of the Korea Institute of Information Security and Cryptology*, 28(1), 249-267.  
DOI : 10.13089/JKIISC.2018. 28.1.249
- [4] Cybersecurity Competency Model.  
<https://www.careeronestop.org/CompetencyModel/competency-models/pyramid-download.aspx?industry=cybersecurity>
- [5] <https://dodcio.defense.gov/Cyber-Workforce/DCWF.aspx>
- [6] William Newhouse, Stephanie Keith, Benjamin Scribner, Greg Witte. NICE Cybersecurity Workforce Framework. NIST SP 800-181.
- [7] NICE Webinar Series 「How You can influence an updates to the NICE framework」  
[https://www.nist.gov/system/files/documents/2019/12/04/NICEFramework\\_Webinar\\_FINAL.pdf](https://www.nist.gov/system/files/documents/2019/12/04/NICEFramework_Webinar_FINAL.pdf)
- [8] D. Yuan. (2017). Design and develop hands on cyber-security curriculum and laboratory. *Computing Conference 2017*. 1176-1179.  
DOI : 10.1109/SAI.2017.8252239
- [9] A. Lodgher, J. Yang & U. Bulut. (2018). An Innovative Modular Approach of Teaching cybersecurity across Computing Curricula. *In 2018 IEEE Frontiers in Education Conference (FIE)*. 1-5.  
DOI : 10.1109/FIE.2018.8659040
- [10] S. Naqvi, P. Sommer & M. Josephs. (2019). A Research-Led Practice-Driven Digital Forensic Curriculum to Train Next Generation of Cyber Firefighters. *In 2019 IEEE Global Engineering Education Conference (EDUCON)*. 1204-1211.  
DOI: 10.1109/EDUCON.2019.8725129
- [11] S. Azadegan & M. O'Leary. (2016) An undergraduate Cyber Operations curriculum in the making: A 10+ year report. *In 2016 IEEE Conference on Intelligence and Security Informatics (ISI)*. 251-254.  
DOI : 10.1109/ISI.2016.7745484
- [13] K. Kim, J. Smith, T. A. Yang & D. J. Kim, (2018). An Exploratory Analysis on Cybersecurity Ecosystem Utilizing the NICE Framework. *In 2018 National Cyber Summit (NCS)*. 1-7.
- [14] N. Miloslavskaya & A. Tolstoy. (2016). State level views on professional competencies in the field of IoT and cloud information security. *In 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*. 83-90.
- [15] Conklin Wm Arthur, Cline Raymond E, Roosa Tiffany. (2014). Re engineering cybersecurity education in the US : An analysis of the critical factors. *System Sciences (HICCS) 47th Hawaii International Conference 2014*. 2006-2014.
- [16] I. Alsmadi & M. Zarour. (2018). Cybersecurity programs in Saudi Arabia: Issues and Recommendations. *In 2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*. 1-5.
- [17] B. D. Caulkins, K. Badillo-Urquiola, P. Bockelman & R. Leis. (2016). Cyber workforce development using a behavioral cybersecurity paradigm. *In 2016 International Conference on Cyber Conflict (CyCon US)*. 1-6.

홍진근(Jin-Keun Hong)

[정회원]



- 1991년 경북대학교 전자공학과(공학사)
- 1994년 경북대학교 정보통신 공학전공(공학석사)
- 2000년 경북대학교 정보통신 공학전공(공학박사)
- 2004년 ~ 백석대학교 ICT학부교수

- 관심분야 : 융합 신기술 및 보안
- E-Mail jkhong@bu.ac.kr