A New Approach to Understand Cybersecurity Workforce Career Path and Its Knowledge, Skills, and Abilities

Abstract – As we are increasingly living in "digital" world, threats to cyber security, such as identity theft, are also on the increase, the need for qualified cyber security professionals is ever increasing; There is currently a shortage of qualified cybersecurity professionals. Outlining the relationships and associative qualifications among cybersecurity job titles, would clarify the progression of knowledge, skills and abilities according to work role classification. This study analyzes the variance in job classifications and job descriptions provided in existing cybersecurity workforce resumes to model career progression. We first analyze the schema regarding industry job titles and work roles utilized by current industry professionals. Then, we propose a model of cybersecurity career pathways based on empirical job transitions and job description data. The proposed model will benefit both cybersecurity professionals to advance their careers and educational organizations to supply qualified cybersecurity professionals by offering the most suitable curriculum.

Keywords

Cybersecurity Professionals, Career Pathways, Job Transitions, Resume Analysis

1. INTRODUCTION

The way we conduct our daily tasks is becoming increasingly digital, even compared to a few years ago: we are banking online, shopping online, communicating online, and so on. With so much information being transmitted and stored online, there come new vulnerabilities such as identity theft, unauthorized access to proprietary information, and ransomware that impact commerce and individual welfare. Although we think we are "safe" because we do not have much of an online presence, even the organizations with which we interact offline are becoming increasingly vulnerable to attacks, where unauthorized access to their data becomes more common as they increasingly transmit data through digital networks or store data in digital clouds. *Identity theft*, for example, is one of the most common and ubiquitous forms of vandalism in the United States. The Bureau of Justice Statistics reported that nearly twice as many identity theft cases were filed in 2016 than all other types of theft combined.[1] According to CIFAS' "The Fraudspace" report, the number of identity theft victims in US has continuously increased. It was 175k cases in 2017, which had been increased 125% in the last decade [**Error! Reference source not found.**]. These threats to cyber security have a significant effect on the organizations as well. According to Cisco, 29% of the breached organizations lost revenue [[4]]. This data has made clear the need for a robust cybersecurity.

Consequently, the need for qualified cyber security professionals is ever increasing. Forbes magazine predicts that the demand of cybersecurity workforce will grow at 10% annually and that annual spending on cybersecurity will reach $170 billion in 2020. In fact, job postings in cybersecurity has tripled in the last three years [**Error! Reference source not found.**]. This surge in demand has made clear the urgency for a structured, one-fits-all linear career map to entering and having a successful career in cybersecurity. The backgrounds and qualifications of current cybersecurity

[1] Victims of Identity Theft, 2016 NCJ 251147. (2019). Bureau of Justice Statistics, US Department of Justice.

professionals vary greatly. Some cybersecurity professionals enter the field directly after college or a graduate degree in a cybersecurity related major, some move from being a generalized IT professional to specializing in cybersecurity, and some enter into cybersecurity from a seemingly irrelevant area but armed with relevant skills.

Another concern regarding professional qualifications is that there are no clearly established guidelines for cybersecurity education standards. The National Security Agency (NSA), in their effort to advance collective cybersecurity skills, have offered to recognize academic institutions that establish robust scholastic programs that grant degrees in cybersecurity. However, the requirements for designation are not tied to any specific ontology, nor do they enumerate a specific progression of knowledge and skills that industry experts would consider benchmarks for mastery performance.

In this light, developing a structured career pathway would help produce the much-needed qualified cybersecurity professionals that will be needed in the future. Career pathways establish a collection of qualification and performance standards that are needed and expected from each cybersecurity position. This is beneficial to both employers and employees alike. Currently, very little is known about how the cybersecurity professionals transitioned into the cybersecurity field and what their career progressions are with work role and required elements including educational, knowledge, skillsets, ability and professional backgrounds most appealing to employers. A study that examines these different paths to successful careers in cybersecurity would help establish benchmarks and guidelines for industry career progression.

In this study, we aim to develop a cybersecurity career path map by answering the following research questions (RQ). *RQ1: What are the key jobs within cybersecurity and common transition opportunities? RQ2: What are the career progressions through work role transitions with detailed required elements (e.g., credentials, skillsets, knowledge, experience) associated with each role? RQ3: How can we map those key elements of cybersecurity workforce to provide some good ways (e.g., career paths for cybersecurity* *professional, a map of cybersecurity certification and KSA, a cybersecurity roadmap, etc.) to serve a basis for helping current and future development of cybersecurity workforce?*

The rest of the paper is organized as follows. Section 2 reviews the previous relevant work and discusses current issues identified in research. Section 3 presents our approach and how our study differs. Section 4 discusses a research method to validate our approach. Section 5 presents preliminary results of the study. Finally, section 6 discuss the findings and practical implications of findings in cybersecurity professional workforce domain.

2. PREVIOUS RELEVANT WORK

A previous study of cybersecurity employment by Brian Fitzgerald et al (2015) noted that the qualifications that employers seek are higher (college) education, certifications and work experience. However, there is limited supply and standardization in terms of education: universities are just now introducing 4-year degree programs in cybersecurity, certifications are not standardized and no-skill/low-skill employment opportunities are difficult to find in the industry. This has left both employers and potential employees in need of a career path denomination in which qualifications and expectations are clearly defined along with the relationship between successive positions.

One source for cybersecurity career pathways is Henry Dalziel's 2015 book, "An Introduction to US Cybersecurity Careers". In it, he familiarizes those interested in joining the industry with the general requirements of cybersecurity professionals as well as guidance on advancing within the cybersecurity industry, such as networking advice and job search resources. He posits two points relative to this research project; 1) Most cybersecurity professionals start their careers in another computer science or IT related field, and 2) The most popular entry-level jobs are "ethical hacker" and "penetration tester".

Another source for cybersecurity career roadmaps is Cyberseek.org. This organization was funded under the NICE initiative to provide an overview of the industry workforce and identify current standards and shortages by both job title and NICE work role. Cyberseek.org uses job market data from burning glass technologies to provide an analysis of employment trends such as positions advertised, positions filled, and the most common certifications requested by employers. Cyberseek.org also provides an overview of cybersecurity career pathways according to job title and organized by career level.

Several government agencies such as NSA, NIST, and DoD have developed top-down standards and guidance on the skills required for this evolving profession. Professional organizations such as SANS, $(ISC)^2$, ISACA, etc., and many business corporations such as CISCO, Microsoft, SharePoint, Citrix, etc., all provide their own sets of certifications related to cybersecurity training and education. In fact, the number and varieties of cybersecurity-related certifications are overwhelming. This issue causes confusion among not only laypersons, but also those IT workers that are seeking cybersecurity certifications to strengthen their own technical qualifications. Furthermore, employers are often confused as well concerning what cybersecurity knowledge, skills, abilities (KSA) and certifications their employees should be equipped with or encouraged to pursue.

In addition, private institutes that offer cybersecurity training and certification also provided career pathways, or at least an organized progression of knowledge, skills and abilities corresponding to their certification offerings. CompTIA, a major provider of cybersecurity technical training and certification, claims to have organized their certification offerings based on career pathways. SANS/GIAC is another training and certification institute that offers its own career pathway that is aligned with the recommended education/certification progression. The international council of e-commerce consultants (EC-Council) is another organization that has organized their training and certification products to represent their ideal career progression where basic and broad qualifications are recommended or required before moving on to more technical and specialized training. While these certifications are not associated with specific job titles, they can be representative of career progression in our study.

As it is evident from the current confusion in cybersecurity workforce, an empirical study of career advancement along with the qualifications of cybersecurity professionals would strengthen employment utility within the industry. Although existing cybersecurity workforce studies provide theoretical structure, an empirical positivist study has yet to be published and would contribute to cybersecurity workforce literature.

3. CYBERSECURITY CAREER PATH FRAMEWORK

3.1 A New Approach to Understand Cybersecurity Workforce Career Path

In such a high-demand area, extensive research has been conducted on this subject. However, previous research has focused on the top-down approach, as opposed to bottom-up.[2] Top-down approach allows us to have a streamlined view into the research area. However, with a top-down approach, we may lose the sight of important empirical details that may better explain the research area and allow us greater academic understanding of the industry.

In a bottom-up approach, we analyze the details of the individuals, such as their educational and professional background, their transition to cybersecurity, and build the major career paths based on these different backgrounds. Therefore, our study provides a much-needed and thorough ontology of what kinds of paths represent a successful career in cybersecurity. Considering both approaches, we can better identify what current KSAs and cybersecurity certifications are predominantly obtained by current cybersecurity professionals and what types of KSA are missing. As a result, we can improve

[2] The top-down approach was developed in 1970s by IBM researchers to create a more efficient system/software development process. It gained popularity in various industries and business management quickly.

future workforce efficiency by identifying what KSAs are needed and encouraged to pursue.

3.2 Cybersecurity Workforce Job Classifications

In order to create a useful and approachable career road map, a hierarchy of positions should be produced according to the most commonly seen job titles in the cyber security industry. Considering both approaches, in this study we propose cybersecurity job classifications as two levels (general and sub-level) and identify the trend of job transactions using a set of posted cybersecurity professionals' curricula vitae. To do so, we identify nine general job titles and a hypothesized career progression in the cybersecurity workforce domain in terms of job experience and cybersecurity work roles. Job experience is based on the levels of cybersecurity knowledge/skills/ability from entry-level positions such as security technicians/specialists to senior/executive-level positions such chief information security officer (CISO). In regard to cybersecurity work roles, we adopt seven work roles (i.e., securely provision, operate & maintain, protect & defend, analyze, collect & operate, investigate, and oversee & govern) from the NICE framework.[3]

Figure 1 presents how work roles within the NICE framework require progressively greater levels of ontological acumen and responsibility according to categorization along with job experience. As a professional progresses in his or her career, they hold positions that require more specialized knowledge/skills/ability along with a generalized understanding of the theories and processes across the different work roles to support cybersecurity goals. Entry level positions/work roles may require a greater degree of technical expertise, but does not include strategic or policy-level decision-making. They operate and maintain existing security systems and protocols but do not influence policy. Oversight and governance, on the other hand, requires little

[3] The NICE Cybersecurity Workforce Framework (NCWF) is a popular guideline for organizing the work roles within the cybersecurity industry according to common knowledge, skills, abilities, and tasks. It consists of seven categories and 33 specialty areas.

technical expertise but a large degree of managerial and policy implementation aptitudes. We expect that this type of progression should be represented in the empirical data that will be analyzed in this study.

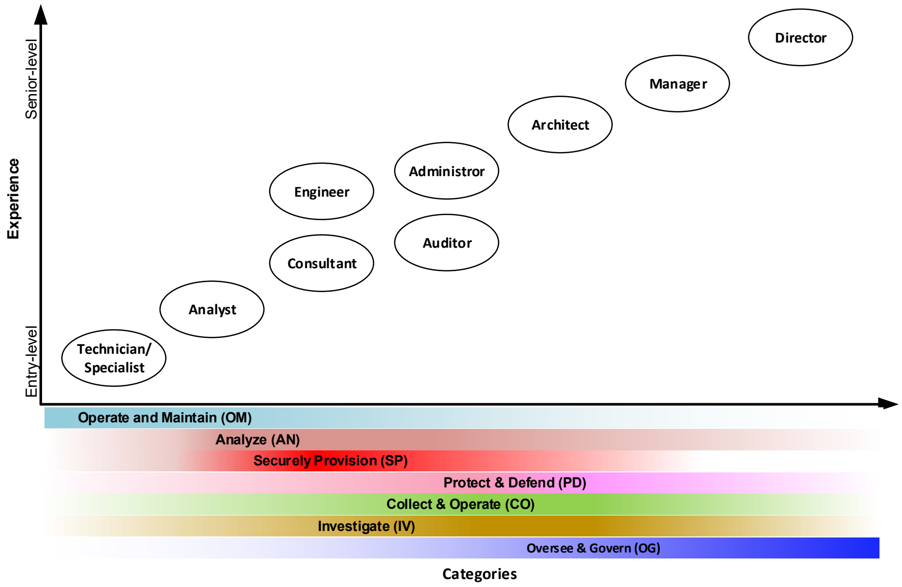


Figure 1. Security Job Classifications

As an empirical data, a curricula vita is a written overview of an individual's professional experience and other qualifications that helps the hiring managers identify preferred candidates for employment. Although there is no single correct format, typically, it describes education, certifications, areas of expertise, professional experience, skills, professional associations/memberships, professional leadership and activities, professional presentations, publications, awards/honors/fellowships, and others.

4. RESEARCH METHODOLOGY

4.1 Data Preparation

To collect cybersecurity professionals' curricula vitae or resumes, we searched nation-wide job posting websites and identified "indeed.com" as one of the leading jobsites for the professionals looking for their next roles. Thus, indeed.com is a good representative of the cyber-security professional who are active in the work force and looking for their next roles that will challenge them and help them grow professionally. We had collected more than 1,200 CVs of cyber security professionals from. Although "indeed.com" allows us to search a whole set of job postings of cybersecurity professionals, the data are anonymous because there is no private identifiable information (PII) posted. The data we captured include their job history, educational background, technical and soft skills, certifications, and other information that may be highly relevant such as military background, security clearance.

After downloading the data using search key words such as "cybersecurity" and "information security", we coded the data and stored it in MS Access as the main database for the study. For the human coding process, four researchers collected and coded the data using a predefined coding protocol. So, as part of coding and data hygiene, we ensured that the data were coded in a consistent way across all coders. The main database consists of four tables (see Figure 3)*:* *Resume, JobExperience, Degree,* and *MilitaryServices*.

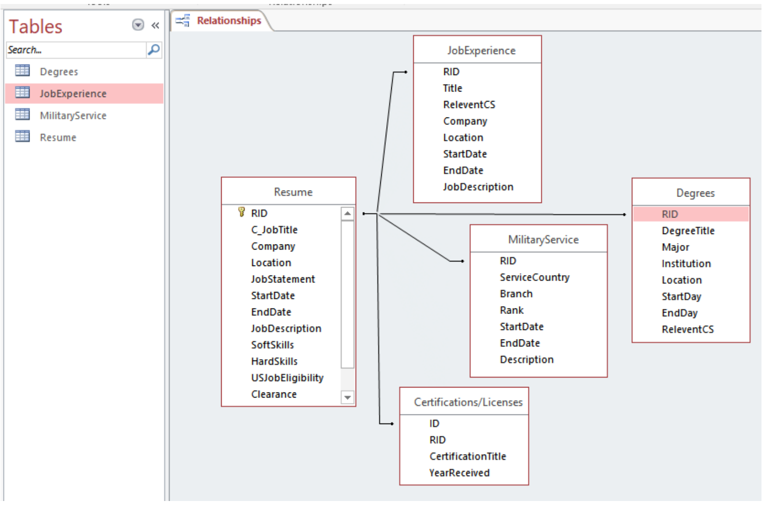


Figure 3. Resume and JobExperience Database

In *Resume* table, we have the current job information (job title, job description, how long they have been in this job, what company and geographic location) and information such as skill set (hard and soft skills), certifications, and security clearance. In *JobExperience* table, we capture their previous job history in detail: Job title, company, dates, location, and tasks performed. Similarly, in *Degrees* table, we capture their educational background in detail: Their degree(s) (BS/MS/Associate, etc.), major, university, dates, whether their major is relevant to cybersecurity. We also capture whether these professionals had military background in *MilitaryService* table: Dates, their rank, branch, and description of their military service. After removing redundant, incomplete and inappropriate, the total number of resumes was 1047 with 5208 positions.

4.2 Data Analysis

The first level of analysis provides an overview of the data that we had collected. In order to understand how the cybersecurity workforce and job transitions should be classified, we needed to determine the level of variance among job titles and task descriptions. Table 1 contains the most commonly used job titles and each variant of it encountered in the data. We will then perform an exploratory factor analysis to test the level of information that can be extracted from the data using ANOVA or other quantitative method. If job tasks provided in the job descriptions covary to a degree that significant clustering occurs, then career progression could be mapped using these data parameters.

5. PRELIMILARY ANALYSIS RESULT

The following tables shows the distribution of current and previously-held job titles among the three most popular job titles in our sample:

Table 1. Distribution of job title observations for current positions

Analyst	Cyber/IT/Network Security Analyst	Systems Analyst	Assurance Analyst
260	244	14	2
	94%	*5%*	*1%*
Specialist	Cyber Specialist	Information Specialist	Other Specialist
79	45	14	20
	57%	18%	25%
Consultant	Cyber Consultant	Information Consultant	Other Consultant
58	34	6	18
	59%	10%	31%

Table 2. Distribution of job title observations for previously held positions

Analyst	Cyber/IT/Network Security Analyst	Systems Analyst	Assurance Analyst
590	400	163	27
	68%	28%	5%

Specialist	Cyber Specialist	Information Specialist	Other Specialist
231	28	52	151
	12%	23%	65%
Consultant	Cyber Consultant	Information Consultant	Other Consultant
285	48	45	192
	17%	16%	67%

In our initial analysis of job titles, we have combined observations of commonly used job titles into general job types. Our data shows that the most commonly observed job type is Analyst followed by Consultant and Specialist. Further analysis is needed to understand the variation of KSAs that delineate this categorization of job titles.

Expected Results

The expected outcome of this analysis is a Maximum A Posteriori (MAP) Model of the current distribution of cybersecurity workforce positions, based on job descriptions and transitions provided in professional resume data.

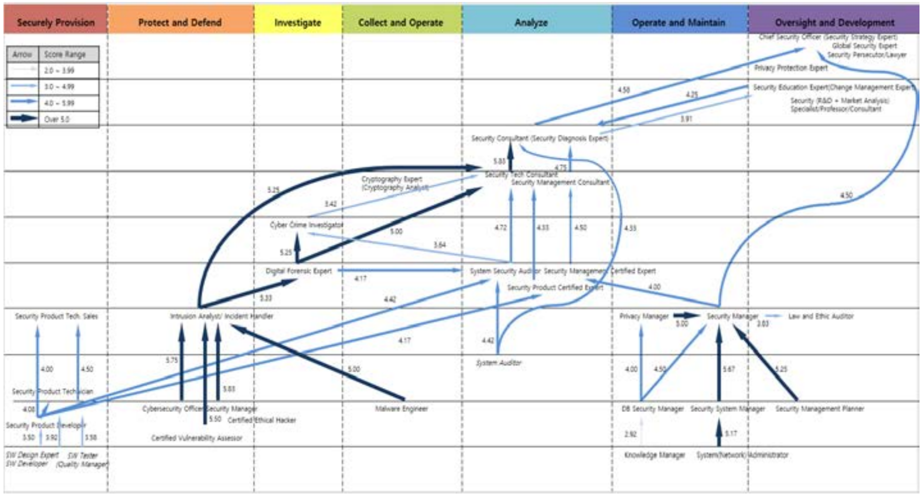

Securely Provision
Protect and Defend
Investigate
Collect and Operate
Analyze
Operate and Maintain
Oversight and Development
Arrow
Score Range
2.0 ~ 3.99
3.0 ~ 4.99
4.0 ~ 5.99
Over 5.0
Chief Security Officer (Security Strategy Expert)
Global Security Expert
Security Persecutor/Lawyer
Privacy Protection Expert
Security Education Expert(Change Management Expert)
Security (R&D + Market Analysis) Specialist/Professor/Consultant
4.58
4.25
3.91
Security Consultant (Security Diagnosis Expert)
5.83
4.75
Security Tech Consultant
Security Management Consultant
Cryptography Expert (Cryptography Analyst)
5.25
3.42
Cyber Crime Investigator
5.00
3.64
5.25
Digital Forensic Expert
4.17
5.33
4.42
4.72
4.33
4.50
4.33
4.50
System Security Auditor
Security Management Certified Expert
Security Product Certified Expert
4.00
Security Product Tech. Sales
Intrusion Analyst/ Incident Handler
4.17
4.42
Privacy Manager
5.00
Security Manager
3.83
Law and Ethic Auditor
4.00
4.50
5.75
5.83
5.00
System Auditor
4.00
4.50
5.67
5.25
Security Product Technician
4.08
Security Product Developer
Cybersecurity Officer
Security Manager
5.50
Certified Ethical Hacker
Malware Engineer
DB Security Manager
Security System Manager
Security Management Planner
3.50
3.92
3.58
Certified Vulnerability Assessor
2.92
5.17
SW Design Expert
SW Developer
SW Tester (Quality Manager)
Knowledge Manager
System(Network) Administrator

Figure 3. Resume and JobExperience Database

6. FINDINGS AND DISCUSSION

The purpose of this research is to model the relationship between job descriptions/qualifications and job transitions of existing cybersecurity professionals. Ideally, the empirical career pathways recognized in this model will provide guidance for aligning academic curriculum and certification progression with existing work roles and profession acumen. Additionally, this model will identify leverage points among qualifications and work roles so that shortages in specific work roles can be addressed efficiently from the existing workforce.

These cybersecurity career pathways will give current cybersecurity job candidates and professionals a better understanding of the skills needed for cybersecurity careers. The cybersecurity certification and course roadmap will help academic institutions and training providers develop relevant training content for cybersecurity courses and certifications. The cybersecurity roadmap will provide employers with clear skill requirements to use for recruitment, selection, and workforce development. It is expected that the discussion based on this research will strengthen the readiness of current and future cybersecurity workforce.

Our study contributes significantly to the area of cybersecurity professionals' career map research in terms of our approach to better understanding the background of a cyber-security professional. We consider a bottom-up approach and study their background and how they become a cyber-security professional (i.e. their educational background, their previous roles before becoming a cyber-security professional, if any, and how they transitioned into the cyber-security industry.) Consequently, based on our observations on the current trends in educational and professional background and popular transition paths, we are able to provide the cybersecurity community with recommendations on how best to supply qualified cybersecurity professionals in terms of curriculum, certifications, and other educational content, as well as guidelines for current cybersecurity candidates and professionals on best professional transition paths to successful careers in cybersecurity.

REFERENCES

[1] FCC. Preserving the Open Internet Broadband Industry Practices, GN Docket No. 09-191, WC Docket No. 07-52, Report and Order, 25 FCC Rcd 17905 (2010).

[2] Victims of Identity Theft, 2016 NCJ 251147. (2019). Bureau of Justice Statistics, US Department of Justice.

[3] Security Intelligence Website, https://securityintelligence.com/news/new-fraud-statistics-show-rising-volume-of-identity-theft/, last accessed 2019/02/22.

[4] Cisco Website, http://b2me.cisco.com/en-us-annual-cybersecurity-report-2017, last accessed 2019/02/22.

[5] Burning Glass Technologies Research Website, https://www.burning-glass.com/research-project/cybersecurity/, last accessed 2019/02/22.

[6] Author, F.: Contribution title. In: 9th International Proceedings on Proceedings, pp. 1–2. Publisher, Location (2010).

[7] Kim, J. and Angakoon, P. (2016). Research using job advertisements: A methodological assessment. Library and Information Science Research.

[8] Hoffman, M., Bach, F., Blei, H. (2010). Online Learning for Latent Dirichlet Allocation. Neural Information Processing Systems (NIPS) conference proceedings.

[9] D. Blei, A. Ng, and M. Jordan. Latent Dirichlet allocation. Journal of Machine Learning Research, 3:993–1022, January 2003.

[10] Vulic I., De Smet W., Tang J., Moens M.-F. (2015). Probabilistic topic modeling in multilingual settings: An overview of its methodology and applications. Information Processing and Management, 51 (1), pp. 111-147.

APPENDIX A. SECURITY JOB TITLES AND RELATED ELEMENTS (EXAMPLE)

Job Title: Security Technician/Specialist

Description:

- Designs, tests, configures, and monitors security controls for systems and networks
- Defends systems against unauthorized access, modification, and/or destruction
- Performs vulnerability testing, risk analyses, and security assessments
- Identifies system and network abnormalities and reports violations
- Responds immediately to security incidents and provides post incident analysis

Related job titles:

- Information Security Specialist
- Cyber Security Specialist
- Computer Security Technician
- Network Security Specialist

NICE relevant factors:

Specialty Area:

Desired K/S/A:

Knowledge:

- TCP/IP, computer networking, and routing and switching
- Windows, Unix, and Linux operating systems
- Security technologies and processes: IDS/IPS, penetration and vulnerability testing, DLP, and anti-malware
- Understanding of ISO 27001/27002, ITIL, and COBIT frameworks
- Familiarity with PCI, HIPAA, GLBA, and SOX compliance assessment

Skills:

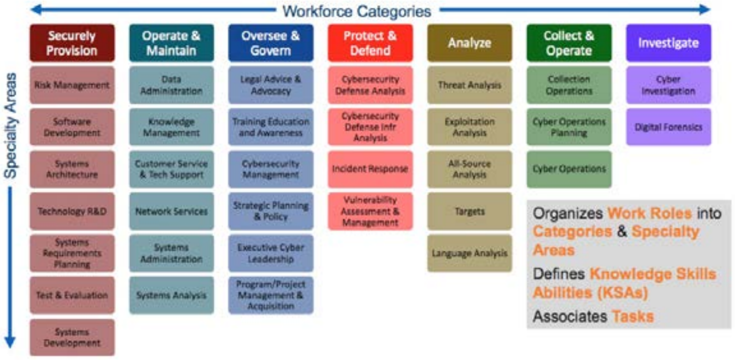
Abilities:

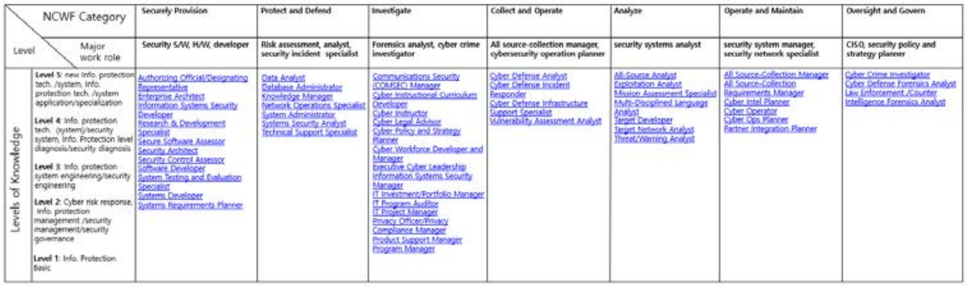
Desired Certifications:

- CompTIA A+, Network+, and Security+, CCNA, CEH, GIAC certifications (GSEC, GCIH, and GCIA), CISSP

APPENDIX B. WORKFORCE CATEGORY, MAJOR WORK ROLE, SPECIALTY AREAS, KNOWLEDGE, AND JOB TITLES (EXAMPLE)[4]

The NICE cybersecurity workforce framework provides an overview of the types of roles a cybersecurity professional may play within an organization. Each category represents a separate collection of skills that is unique to that work role type. For example, the *Securely Provision* category contains work roles that support operations through implementing security measures and procedures for an organization. While this framework organizes work roles into specialty areas and categories based on common tasks and skills, it does not provide a transitional map from entry level to terminal positions. Empirical evidence would provide a better understanding of the distribution of knowledge, skills and abilities among cybersecurity positions along with job transitions typically seen among the existing workforce.





NCWF Category		Securely Provision	Protect and Defend	Investigate	Collect and Operate	Analyze	Operate and Maintain	Oversight and Govern
Level	Major work role	Security S/W, H/W, developer	Risk assessment, analyst, security incident specialist	Forensics analyst, cyber crime investigator	All source-collection manager, cybersecurity operation planner	security systems analyst	security system manager, security network specialist	CISO, security policy and strategy planner
Levels of Knowledge	Level 5: new Info. protection tech. /system, Info. protection tech. /system application/specialization Level 4: Info. protection tech. (system)/security system, Info. Protection level diagnosis/security diagnosis Level 3: Info. protection system engineering/security engineering Level 2: Cyber risk response, Info. protection management /security management/security governance Level 1: Info. Protection Basic	Authorizing Official/Designating Representative Enterprise Architect Information Systems Security Developer Research & Development Specialist Secure Software Assessor Security Architect Security Control Assessor Software Developer System Testing and Evaluation Specialist Systems Developer Systems Requirements Planner	Data Analyst Database Administrator Knowledge Manager Network Operations Specialist System Administrator Systems Security Analyst Technical Support Specialist	Communications Security (COMSEC) Manager Cyber Instructional Curriculum Developer Cyber Instructor Cyber Legal Advisor Cyber Policy and Strategy Planner Cyber Workforce Developer and Manager Executive Cyber Leadership Information Systems Security Manager IT Investment/Portfolio Manager IT Program Auditor IT Project Manager Privacy Officer/Privacy Compliance Manager Product Support Manager Program Manager	Cyber Defense Analyst Cyber Defense Incident Responder Cyber Defense Infrastructure Support Specialist Vulnerability Assessment Analyst	All-Source Analyst Exploitation Analyst Mission Assessment Specialist Multi-Disciplined Language Analyst Target Developer Target Network Analyst Threat/Warning Analyst	All Source-Collection Manager All Source-Collection Requirements Manager Cyber Intel Planner Cyber Operator Cyber Ops Planner Partner Integration Planner	Cyber Crime Investigator Cyber Defense Forensics Analyst Law Enforcement /Counter Intelligence Forensics Analyst

[4] Source: www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework