Exploring How the NICE Cybersecurity Workforce Framework Aligns Cybersecurity Jobs with Potential Candidates

Adriane C. Estes[1], Dan J. Kim[2], and T. Andrew Yang[3]
[1]Computer Information Systems, University of Houston-Clear Lake, Houston, Texas, USA
[2] Information Technology & Decision Sciences, University of North Texas, Denton, Texas, USA
[3] Computer Science, University of Houston-Clear Lake, Houston, Texas, USA

Abstract - *We discuss the NICE Cybersecurity Workforce Framework (NCWF), and its role in aligning cybersecurity jobs with candidates. As a workforce development tool, the NCWF can contribute to better retention, reduced new hire training, and cybersecurity education development. The effectiveness of the NCWF, however, requires discretion from hiring managers, academics, and job seekers. Through skills mapping and calibration, the NCWF helps to identify and resolve skill deficiencies; as a framework of core competencies for cybersecurity jobs, the NCWF helps employers to write job descriptions understood by applicants. We first review the NCWF, and then explain how it may enable mapping between jobs and qualifications. We also discuss the effects of job mapping on organizations and candidates, and its long-term benefits.*

Keywords: NICE, NCWF, Cybersecurity, Workforce, Mapping

1. Introduction

The National Initiative for Cybersecurity Education (NICE) is a division of the National Institute of Standards and Technology (NIST). NICE works with the public and private sectors, academia, and the federal government to “improve solutions to a wide range of technical and policy cybersecurity challenges.” [1] In 2014, the NICE Cybersecurity Workforce Framework (NCWF) 2.0 was made available to the public. Participation was initially voluntary but encouraged. In August 2015, the Federal Cybersecurity Workforce Assessment Act was passed, requiring Federal agencies to use the NCWF to “create a consistent framework to expedite the recruitment of highly qualified personnel” for information technology and cybersecurity roles. [2]

This article discusses the NICE Cybersecurity Workforce Framework’s role in workforce development. The NCWF can be used for workforce development through education and training programs, helping to determine what materials are useful at various organizational levels and allowing tailored adoption of the framework. Additionally, students and entry-level workers can use the NICE Cybersecurity Workforce Framework for career planning. A set of clearly defined standards helps individuals decide where to focus their training and specializations by allowing them to see which skills are relevant to their career goals. An update to the NICE Cybersecurity Workforce Framework is currently underway, with an estimated release time of Winter 2018. [3, 4]

In this article, we first introduce the National Institute of Standards and Technology (NIST) and the National Initiative for Cybersecurity Education (NICE), and provide a simplified view of the NICE Cybersecurity Workforce Framework’s structure. We then explain the meaning of mapping, the methodologies used, and how they are applied to the NCWF. We also explain the effects of accurate job mapping on organizations and candidates, and how a wider adoption of the NICE Cybersecurity Workforce Framework may provide long-term organizational benefits through improved recruiting.

2. NIST, NICE, and the NICE Cybersecurity Workforce Framework

The National Institute of Standards and Technology defines its mission as “promot[ing] U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.” [5] Overseen by the U.S. Department of Commerce, the NIST is responsible for defining units of measure and benchmarking industry standards both in the United

States and internationally. Measurement science, or metrology, has a broad domain. Weights and volumes typically come to mind, but metrology also includes industrial and workforce standards. Simply put, if something uses technology or can be manufactured, then NIST has likely contributed to its development at some point.

Part of NIST's vision is to "be the world's leader in creating critical measurement solutions and promoting equitable standards." [5] In a global market, standardized practices are developed to help countries work together more effectively. Without a consensus on industry standards, user safety is jeopardized or trade between nations can be adversely affected. This means that setting industry standards through globalized collaboration not only helps to advance the fields of metrology and technology, but also strengthens international relations and supports economic growth.

No definitive global standard for cybersecurity exists despite a surge in both casual and professional technology use. In 2013, the U.S. government began its own process for standardization when the creation of a Cybersecurity Framework was announced. [3] With decades of experience setting information technology and computing standards, NIST [6] was a logical choice for overseeing the project with its National Initiative for Cybersecurity Education (NICE) already underway. [7]

Since 2010, NICE has worked with the government, public sector, and academia to "cultiva[te] an integrated cybersecurity workforce that is globally competitive from hire to retire". [7] NIST primarily works with risk management for cybersecurity while NICE uses its NICE Cybersecurity Workforce Framework (NCWF) to study the roles and skills of cybersecurity professionals, emphasizing the relationships between workforce development and cybersecurity education. [8] The NCWF is a reference guide that provides a "common lexicon" for describing the knowledge, skills, abilities, and tasks (KSATs) used in the field of cybersecurity and with other jobs which deal with information technology and security. [7]

Seven broad categories form the superstructure of the NCWF. The categories are grouped by work roles within an organization, including S*ecurely Provision*, *Operate and Maintain*, *Oversee and Govern*, *Protect and Defend*, *Analyze*, *Collect and Operate*, and *Investigate*.

Figure 1 depicts the seven categories in a ring format as a reminder that these are system components, not a hierarchy.

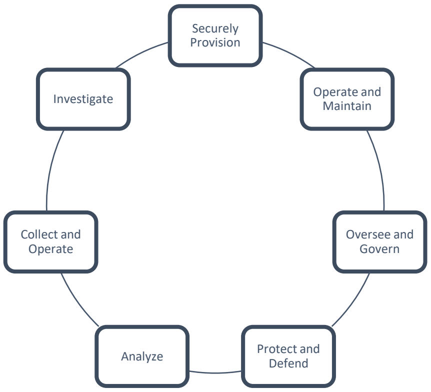


Figure 1: The seven categories of the NCWF [7]

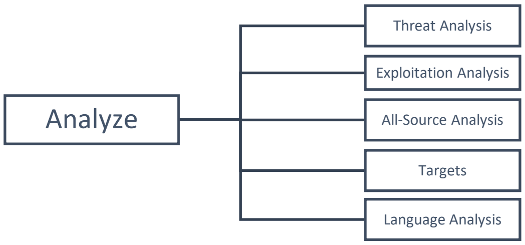


Figure 2: The five specialty areas of the *Analyze* Category [7]

Each category is further divided into specialty areas. Figure 2 shows the five specialty areas that are associated with the Analyze category. A *specialty area* is composed of the essential knowledge, skills, and abilities (KSA) associated with that area. *Task* is another subcategory that has been analyzed and mapped. Some resources list tasks separately from KSAs, but they are included in this analysis and referred to as KSATs. Like KSAs, tasks are also assigned an ID number. Because different jobs can require similar tasks, it is common for a task to be mapped to more than one job title. The National Initiatives for Cybersecurity Careers and Studies (NICCS) has created a downloadable "pushbutton tool" to help hiring managers and human resources specialists sort through the long lists of KSATs [9]. A convenient search feature can also be found on the NICCS's website. For example, a search for task number T0001 [10] gave the following results:

Task ID: **T0001**
Task Description: Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk.

This search mapped T0001 to the following careers:

- Executive Cyber Leadership
- Information Systems Security Manager
- Cyber Workforce Developer and Manager

A comprehensive list of KSATs may be found in Appendix A of the NIST Special Publication 800-181. [7] Additionally, a more detailed and organized view may be found in the NICE Framework 2.0 spreadsheet [4], where every category has its own worksheet, and KSATs are assigned item numbers and descriptions.

The following analyses detail the mapping process and examine how accurately mapping knowledge, skills, abilities, and tasks of cybersecurity jobs using the NICE Cybersecurity Workforce Framework helps organizations recruit qualified candidates.

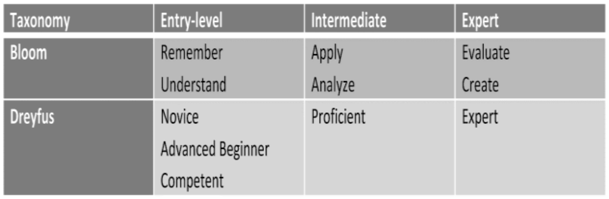
3. Mapping the NICE Cybersecurity Workforce Framework with job functions

The September 20, 2017 NICE Webinar, "Efforts to Align Training and Certifications to the NICE Framework," [11] explained how the NICE Proficiency Team and the NICE Skills-Based Training Certification Project Team conducted skills mapping and its effects on job seekers and employers. This section introduces the concept of mapping, explains mapping methodology, and discusses how mapping may, both positively and negatively, affect the cybersecurity industry.

3.1 Mapping and methodologies

In this analysis, the Oxford Dictionary's definition of mapping will be used. Mapping is defined as "an operation that associates each element of a given set (the domain) with one or more elements of a second set (the range)." [12] A bottom-up view to the NICE Cybersecurity Workforce Framework shows that each KSAT is mapped to a specialty area, and that specialty area is mapped to a category. All seven categories fall under the Cybersecurity career domain.

When the NIST began mapping competencies, one of the framework's original intended uses was cybersecurity risk management, so a combination of existing global standards and best practices were examined. [3] By evaluating the cybersecurity domain as it currently existed vulnerabilities could be identified, leading to the development of more robust training programs to cover those deficiencies. The NICE Skills-Based Training Certification Project Team uses a combination of Bloom and Dreyfus taxonomies. Bloom's taxonomy categorizes skills into six cognitive levels (*Remember*, *Understand*, *Apply*, *Analyze*, *Evaluate*, and *Create*), rated by complexity. Dreyfus' taxonomy uses five skill levels ranging from *Novice* to *Expert*. A matrix was created, shown in Figure 3, blending the two taxonomies. [11] The matrix matches the skill types from the Bloom and Dreyfus taxonomies to career levels (entry-level, intermediate-level, and expert-level). A graphical representation such as this can help employers decide what level of experience they truly need for a position.



Taxonomy	Entry-level	Intermediate	Expert
Bloom	Remember Understand	Apply Analyze	Evaluate Create
Dreyfus	Novice Advanced Beginner Competent	Proficient	Expert

Figure 3: A blend of Bloom and Dreyfus skill set taxonomies [11]

3.2 Agencies who contribute to skills mapping

The NCWF was designed to be used by private "industr[ies], academia, and other government agencies", and the NIST and the Department of Homeland Security's (DHS) Critical Infrastructure Cyber Community Voluntary Program worked together to encourage its adoption. [3] Making the framework available to the public sector provided a "road map" to organizations establishing their own cybersecurity infrastructures. Rather than develop and enforce a set of standards, the early mapping processes involved observing the cybersecurity policies used by industry leaders with the desired candidate skillsets, mapping them, and drawing conclusions based upon the data.

Over time, weaknesses in the NCWF were revealed, and a new purpose for skills mapping was identified. The NICE Proficiency Team's primary objective is to define a mapping "methodology that yields repeatable and validated results." [11] With repeatable results, standardization for KSATs will occur, and the utility of the NICE Cybersecurity Workforce Framework will be increased.

Until 2015, participation and use of the framework was encouraged, but voluntary. [3] On August 6, 2015, the 114th Congress passed the Federal Cybersecurity Workforce Assessment Act. [2] This bill requires all federal agencies to assess their workforce using the NCWF to increase consistency in its use, create a baseline evaluation of the cybersecurity workforce, and identify critical needs. An employment coding structure was added to the NCWF to distinguish civilian from non-civilian cyber personnel.

3.3 The effects of accurately mapped KSATs

Since its implementation, the NICE Cybersecurity Workforce Framework has been used as a guide for classifying and describing work roles in the cybersecurity industry. As KSATs are better defined and calibrated, implementing the NCWF provides benefits for organizations when it comes to recruiting, training, and retention. The following subsections will explain how the NCWF is useful in job recruiting, how candidates benefit from the NCWF, and the long-term effects on organizations and workforce development.

3.3.1 The NCWF as a job recruiting tool

Writing job descriptions in a way that allows job candidates to understand the roles and requirements of the position before applying has a positive effect on recruiting for both the candidate and the employer. [16] By understanding the KSATs required for cybersecurity roles within an organization, employers can recruit more effectively. If, for example, a job description written for an entry-level position requires expert skill sets, the following negative effects could occur:

- A perceived need for job seekers to invest in additional training results in delayed entry into the job market.
- An imbalance between skill sets and hands-on experience.
- Qualified candidates may pass over a job listing because the pay appears too low for the requested skills and experience.
- Academia and private training programs will respond by working to include those skills; such responses extend training time and costs for students and professionals, creating a higher barrier to entry.

Entry-level candidates are simply that—entry level. The matrix in Figure 3 placed the skills needed for entry-level positions on the lower end of the spectrum. Entry-level workers should therefore be expected to demonstrate more practical applications of learned concepts and do less evaluation and content creation. However, that should not automatically lower the desirability for an entry-level candidate. Cultivating an employee's learning potential should instead be considered as an investment by the employer. Clearly and realistically identified skillsets will draw applicants who can meet employers' expectations. [11, 16]

Early in its development, as Ernie Hayden of Securicon noted, the NCWF was "performance based" and not "compliance driven." [17] The risks considered during the development of the framework were provided by volunteers and, consequently, were not representative of all risks across all industries. A tendency to gravitate toward the tech industry was affirmed by Bill Newhouse, Deputy Director of the NICE program, who said, "when identifying their cybersecurity staff, many organizations overlook cybersecurity tasks being performed by lawyers, auditors and procurement officers." [11] Technology is constantly changing, making the job of keeping the NCWF up-to-date an ongoing project. [18] Therefore, the NCWF is not a perfect solution to all recruiting issues, and employers should not blindly rely on it when creating cybersecurity positions. It is imperative for hiring managers, industry leaders, and academia to actively research the skills needed to address a litany of new cyber threats and understand how those skills would benefit their company.

Consistency is perhaps one of the most effective ways to improve the NCWF. Consistency in language, mapping methodologies, participation, and utilization will address the NCWF's current weaknesses. The NICE Cybersecurity Workforce Framework was never intended to be used as a search engine. [11] Its design allows flexibility and encourages employers to use it in a context that best suits their organization's needs. Furthermore, using consistent language throughout the cybersecurity industry when describing KSATs allows educators to better prepare students to enter the workforce and helps improve KSAT mapping.

3.3.2 How skills mapping affects job seekers

Changing jobs is precarious. Even if a job is not a good fit, concerns such as lost wages, a disjointed work history, and losing the time invested in a career are all deterrents to leaving a position. Candidates and hiring managers need ways to evaluate whether a job is a good long-term fit for the candidate. Setting a career path can help take the guess work out of the interview process by facilitating communication between employer and candidate.

Identifying logical career paths has become easier through KSAT mapping. When candidates can determine if a logical career path exists, they can plan their education and personal career goals accordingly [16]. *Cyberseek* [19], a project supported by the National Initiative for Cybersecurity Education, is a useful starting point for cybersecurity career planning. Cyberseek can be combined with the NICE Cybersecurity Workforce Framework, to create a robust tool to aid candidates in deciding which types of cybersecurity jobs they will thrive in and provide a guide for building the appropriate skillset.

The Cybersecurity Credentials Collaborative (C3) is conducting a calibration survey to help higher education and training programs identify relevant cybersecurity skills. [11] C3's goal is to take industry feedback and incorporate it into the types of training used to prepare job seekers. Soft skills and technical skills are both included in this calibration survey along with eliminating overzealous mapping, which is detrimental to the successful application of the framework.

Subject Matter Experts (SMEs) contribute to the mapping process by evaluating required skill levels and competencies. With some mapping efforts aiming at over 90% coverage for a career, this increases the difficulty of creating a repeatable and standardized process. [11] Overworked lists of mapped skills become unmanageable, unrealistic, and overwhelming. Therefore, it is important to consider the scale of how KSATs are mapped to a position. Mapping too many KSATs to any position creates a scenario where every candidate must possess an intermediate or expert skill set, effectively edging out promising entry-level candidates. [11] To avoid over-mapping, the following points should be kept in mind:

- Needs vs Wants: Are the *needs* of a position understood and planned for? How will the *wants* of a position benefit the organization?
- Feasibility: Are the SMEs only considering the expert level skills or are their own skill levels affecting how the position is mapped? Is there a realistic way for applicants to possess or gain all the KSATs described?
- Relevancy: Are the desired KSATs even relevant to the position? Which certifications will adequately satisfy the needs of the position?

Calibration streamlines skills mapping by focusing on what is essential to the work roles. This standardization of core competencies lowers the barrier of entry for future cybersecurity professionals. The primary benefit to candidates is that they can devote time to training to meet the baseline needs of a work role, before investing time in meeting the specialized wants that are often unique to each organization. Over time, these calibration efforts will continue to benefit job seekers as businesses and academia make adjustments based on the calibration results.

3.4 Organizational effects

After conducting cybersecurity workforce studies, the NICE Skills-Based Training and Certification Project Team observed the following:

> "[T]he three most common skill deficiencies are communication skills, business knowledge, and technical skills to provide vendor agnostic skills-based training and performance certification guidelines and tools assisting with problem definition, gap analysis, analytics, and solution sets." [11]

While mapping KSATs has identified these areas for improvement, both employers and training programs share the responsibility for these skill deficiencies. Some of the deficiencies listed are soft skills, and others are related to applied critical thinking. Contributions to the NCWF and its mapping efforts provide valuable industry feedback. That feedback is used by academia and private training programs to design the curricula which prepares candidates for the job market. Therefore, the most direct route to correcting these deficiencies is to improve how employers define job descriptions. Writing job descriptions holistically, including both soft and technical skills, can be as important as determining the proficiency level.

Misstating proficiency adversely affects competency mapping. Sometimes job descriptions are written in a way that overlooks the baseline skills needed for a position. In other words, the job does not fit the description. Subject matter experts have contributed to mapping skills needed by the private sector, but a tendency to focus on the expert level skillsets and neglect the entry-level skills was observed. In the September 20th 2017 NICE Webinar, Jeff Frisk called the phenomenon the "*rush to the top*", which can result from emphasizing the wants, or variable skills, of a position over its needs, or baseline skills. [11]

For example, consider a company that needs an entry-level position such as a Cybersecurity Specialist, but writes a job posting asking for skills that are needed by a Cybersecurity Engineer, an expert level position. The intentions may be perfectly innocent. Perhaps a younger organization wants to hire an employee who can survive its growing pains. Maybe a busy hiring manager did a web search to find a general skill set to write a hiring ad for another department. Either way, it is unlikely the employee will be a good fit in the long run.

An entry-level job description that describes an intermediate-level position will draw applicants who are somewhat overqualified for a position's daily needs. When a mismatch is found between entry level and expert level, the detrimental effects are increased. Not only will applicants be overqualified but, if the salary is set for an entry-level position, the difficulty of hiring will certainly increase. Worst of all, if an employer relies on market estimates to determine salary and does not understand which level they should hire for, they could be paying for an expert when an entry-level employee would meet the organizational needs. [16] Therefore, it is important for employers to be realistic in their expectations, consider the job fit, and understand what skills they need for their organization.

Considering these points builds a foundation for more effective recruiting, training and staff development over time. Incorporating these points into hiring practices can increase employee retention and reduce turnover. The NICCS and DHS created the following graphic (Figure 4) [9] illustrating how effective recruiting builds a robust workforce:

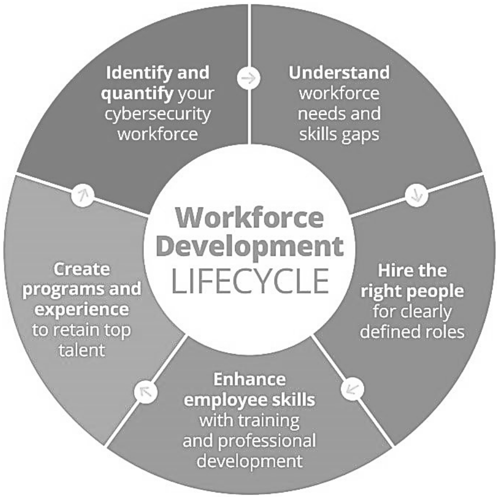

Workforce Development LIFECYCLE
Identify and quantify your cybersecurity workforce
Understand workforce needs and skills gaps
Hire the right people for clearly defined roles
Enhance employee skills with training and professional development
Create programs and experience to retain top talent

Figure 4: The workforce development life cycle [9]

The workforce development lifecycle begins with identifying the needs of the workforce, and its remainder is devoted to training and employee retention. Regardless of their existing skillset, training and retaining new employees require time and funds. The Wall Street Journal reported that the estimated cost of replacing a new hire is “upwards of twice an employee’s salary.” [16] This investment risk falls squarely on the organization. Once again, the reduction of new hire turnover rates can be traced back to understanding the needs of the organization. Reduction in new hire training allows more investment in current staff [20], including competitive wages. According to The Wall Street Journal and Forbes, employee dissatisfaction is reduced when employees feel stimulated. [16, 21] As the retention grows, the workforce development cycle begins again, but with more existing personnel. Training becomes more efficient by reducing the number of hours spent on certifications that may not actually be useful for the organizational role.

4 Conclusion

Mapping job skills to the NICE Cybersecurity Workforce Framework helps to identify skill deficiencies that exist in the cybersecurity industry, and aids in the development of global cybersecurity workforce standards. A combination of industry feedback and skills mapping calibration assists in developing training programs to prepare future cybersecurity professionals that will address those deficiencies.

The cybersecurity field provides endless opportunities to learn and grow. However, there is a difference in personal growth and being overwhelmed with a litany of tasks. Mapping can assist in developing career paths for employees, including training and certifications, giving employees the tools needed to achieve their career goals over time. The NICE Cybersecurity Workforce Framework allows employers to identify their organizational needs and seek candidates who are the right fit for the job, reducing turnover and increasing retention rates. As a result, candidates will be better aligned with job opportunities in the cybersecurity industry. However, the NCWF should not be used as a cure-all for all recruiting issues, because its design is process driven and new cyber threats arise daily. Therefore, while the NCWF is a useful starting point for evaluating organizational cybersecurity needs, it is still necessary to use discretion when determining the KSATs of positions and when developing or choosing training programs.

Acknowledgments

This research has been supported by the National Science Foundation (under grant #1723596) and by the National Security Agency (under grant # H98230-17-1-0355).

References

[1] (2018). *National Initiative for Cybersecurity Education (NICE)*. Available: https://www.nist.gov/itl/applied-cybersecurity/nice

[2] *S.2007 - 114th Congress (2015-2016): Federal Cybersecurity Workforce Assessment Act*, 2018.

[3] (2017). *Launch of the Cybersecurity Framework*. Available: https://obamawhitehouse.archives.gov/the-press-office/2014/02/12/launch-cybersecurity-framework

[4] (2017). *DRAFT Special Publication 800-16 Revision 1 (2nd Draft, Version 2), A Role-Based Model for Federal Information Technology/Cyber Security Training - draft_sp800_16_rev1_2nd-draft.pdf*. Available: https://www.nist.gov/sites/default/files/documents/2017/09/06/draft_sp800_16_rev1_2nd-draft.pdf

[5] (2018). *NIST Mission, Vision, Core Competencies, and Core Values*. Available: https://www.nist.gov/about-nist/our-organization/mission-vision-values

[6] (2018). *Cybersecurity Framework FAQS Framework Basics*. Available: https://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-basics

[7] U.S. Department of Commerce. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework - NIST.SP.800-181.pdf*. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

[8] (2018). *Strategic Plan*. Available: https://www.nist.gov/itl/applied-cybersecurity/national-initiative-cybersecurity-education-nice/strategic-plan

[9] (2018). *DHS PushButtonPD™ Tool | National Initiative for Cybersecurity Careers and Studies*. Available: https://niccs.us-cert.gov/workforce-development/dhs-pushbuttonpd-tool

[10] (2018). *Tasks | National Initiative for Cybersecurity Careers and Studies*. Available: https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework/tasks?name_selective=T0001&description_selective=All

[11] National Initiative for Cybersecurity Education (NICE), "Efforts to Align Training and Certifications to the NICE Framework: September 20, 2017," in *NICE Webinar Series*, ed, 2017.

[12] "mapping | Definition of mapping in English by Oxford Dictionaries," ed, 2018.

[13] "Writing Cybersecurity Position Descriptions for the Greatest Impact_19," ed, 2018.

[14] (2017). *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. Available: https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

[15] "Cybersecurity Framework FAQs Using The Framework," ed, 2018.

[16] T. W. S. Journal. (2018, 2/25/2018). *How to Reduce Employee Turnover - Management - WSJ.com*. Available: http://guides.wsj.com/management/recruiting-hiring-and-firing/how-to-reduce-employee-turnover

[17] T. Network, "NIST cybersecurity framework: Assessing the strengths and weaknesses," S. Security, Ed., ed, 2018.

[18] D. Lohrmann. (2018, 2018/03/02). *NIST Cybersecurity Framework: Five reasons why it matters for your infrastructure*. Available: http://www.govtech.com/blogs/lohrmann-on-cybersecurity/NIST-Cybersecurity-Framework-Five-reasons-why-it-matters-for-your-infrastructure.html

[19] (2017). *Cybersecurity Career Pathway*. Available: http://cyberseek.org/pathway.html

[20] R. K. Mobley. (2018, 2/23/18). *Workforce Development Is No Longer Optional*. Available: https://www.lce.com/Workforce-Development-Is-No-Longer-Optional-1298.html

[21] (2018). *Seven Ways To Increase Employee Satisfaction Without Giving A Raise*. Available: https://www.forbes.com/sites/joefolkman/2013/11/27/seven-ways-to-increase-employee-satisfaction-without-giving-a-raise/#46fd9afe4bb9