**Cybersecurity Staffing**

Jose Flores

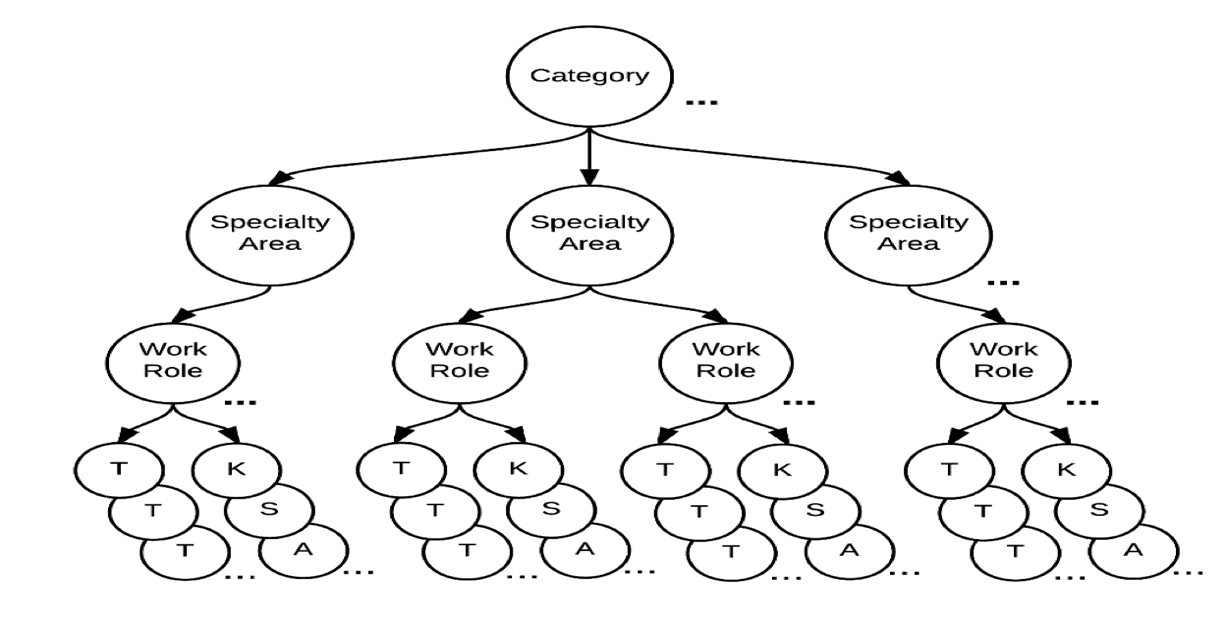
CSOL-550-01-FA22: Management and Cyber Security

Dr. William Hess

December 5, 2022

**Cybersecurity Staffing**

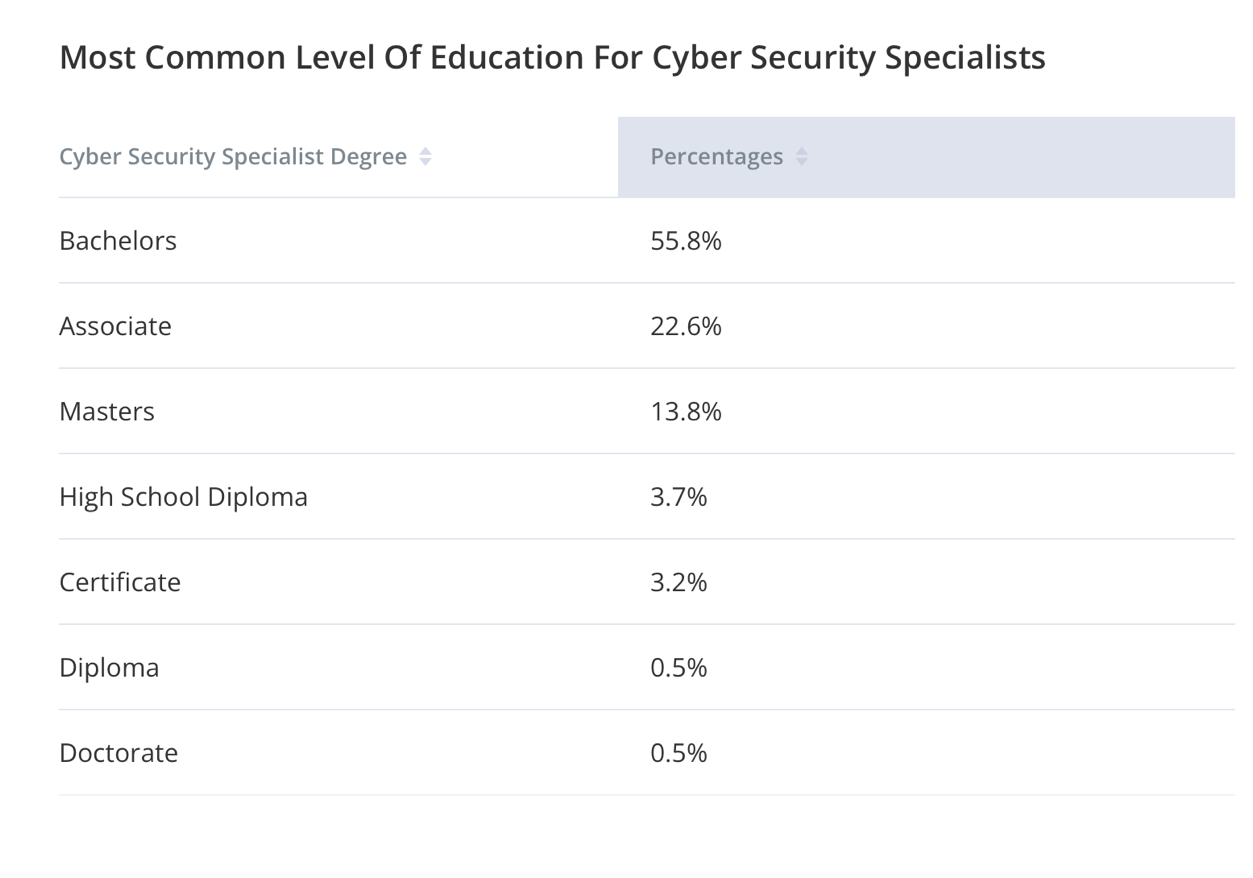
Building a successful cybersecurity team involves knowledge, skills, and abilities (KSAs). The organization’s mission statement will determine the personnel needed to meet those standards. The cybersecurity industry has been increasing throughout the years. Organizations spent about $150 billion in 2021 on cybersecurity resulting in a 12.4% annual increase (Aiyer, Caso, Russell, & Sorel, 2022). The National Institute of Standards and Technology developed the National Initiatives for Cybersecurity Education (NICE) framework highlighting different categories of fields in cybersecurity. These categories fields are Securely Provision (SP), Operate and Maintain (OM), Oversee and Govern (OV), Protect and Defend (PR), Analyze (AN), Collect and Operate (CO) and Investigate (IN) (NIST, 2017). The NICE framework further breaks down the categories into specialty areas and work roles such as software developer, system administration, and executive cyber leadership. Each category can be fulfilled with different levels of experience; however, the organization can increase the requirements to meet its standards. Using the NICE framework will help build a successful cyber staff by identifying work roles fitted with the correlating attributes an organization seeks.



(NIST, 2017)

**Education Levels**

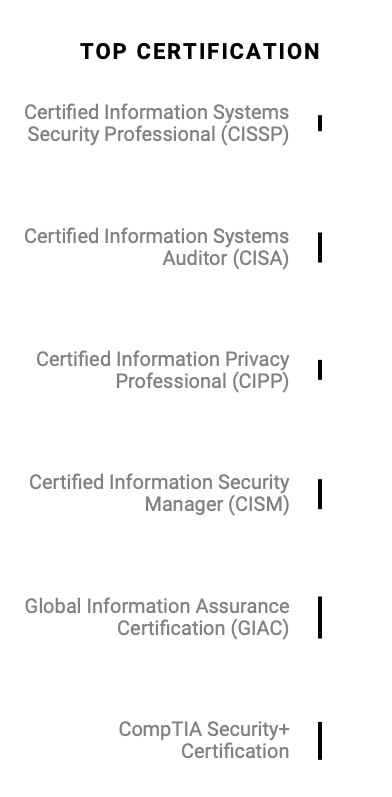
Different-level careers require a vast combination of KSAs and characteristics. Senior-level employees will have a different mindset than entry-level employees due to their years of KSAs and career development. According to Indeed (2022), education, certification, experience, and skills are requirements for an entry-level cybersecurity job. Meeting the education level in cybersecurity depends on what category field you will be working in. Dr. Moore, an academic director at the University of San Diego, further explains that an “entry-level,” according to the National Security Agency (NSA), is defined as a Bachelor’s degree with three years of relevant experience, Master’s degree with one year of relevant experience, Doctoral degree with no experience or an Associate’s degree with five years of extensive experience in the position (2022). A cybersecurity specialist usually has a bachelor's degree rather than other degrees (Zippia, 2022).



(Zippia, 2022)

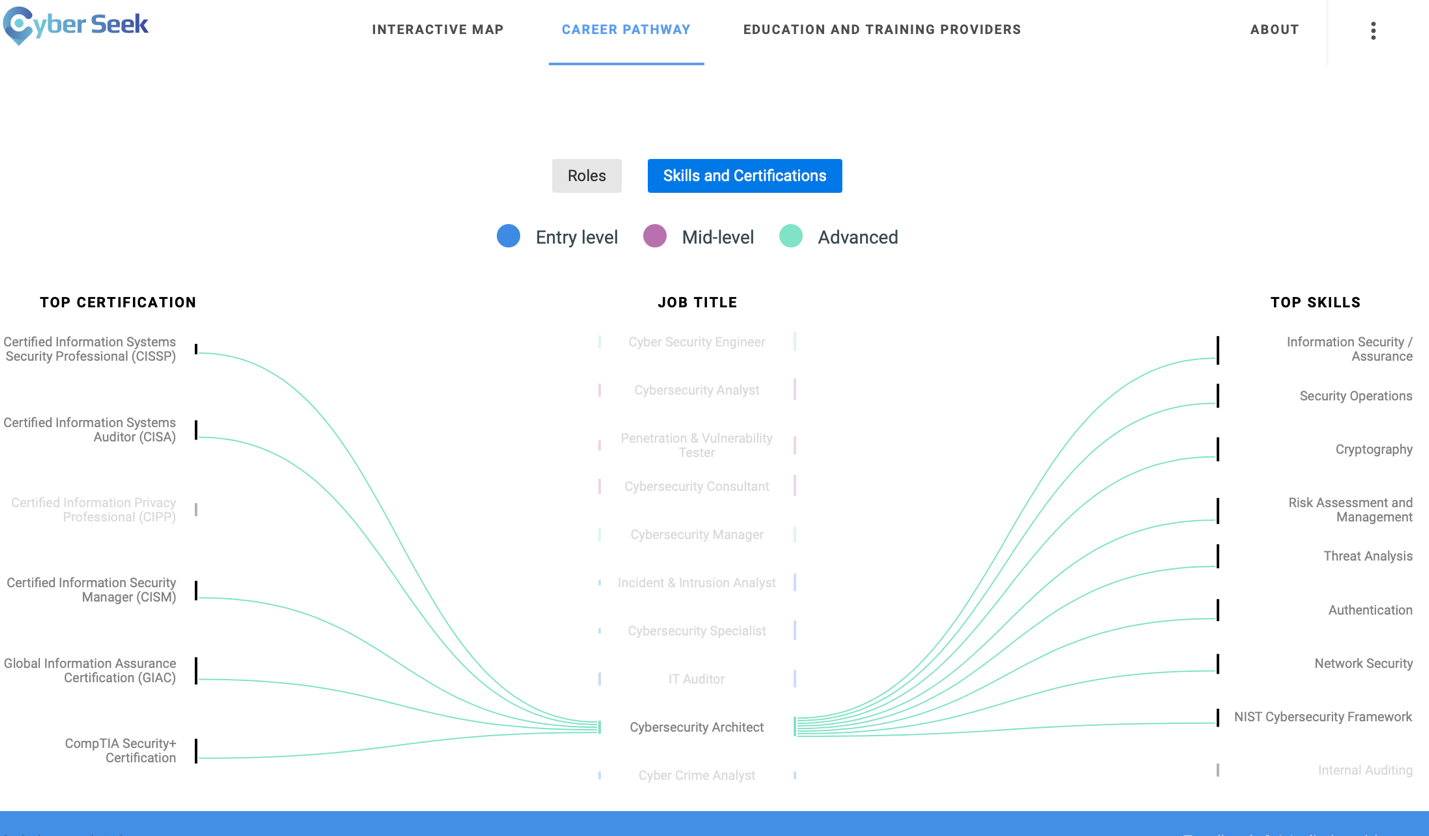
**Certifications**

Entry-level jobs require a different level of education, and some organizations will accept certification instead. A certification is an official document that proves the title holder has completed an educational course and demonstrated the skills and abilities to perform in the respected field. Popular cybersecurity certifications are CompTIA Security+, GIAC Security Essentials, Certified Ethical Hacker, and Cisco Certified Cyber ops (Uche, 2022). Depending on the work role will depend on what certification an individual should earn. Mid-level professional careers, such as cybersecurity analysts, require at least five years of experience (Uche, 2022). Higher-level professional careers, such as Chief Information Security Officer (CISO), require 12-15 years of experience, multiple certifications, and a wide range of skills (Rand, 2022). Cyberseek (2022) identified the top certifications and skills depending on cybersecurity job titles.

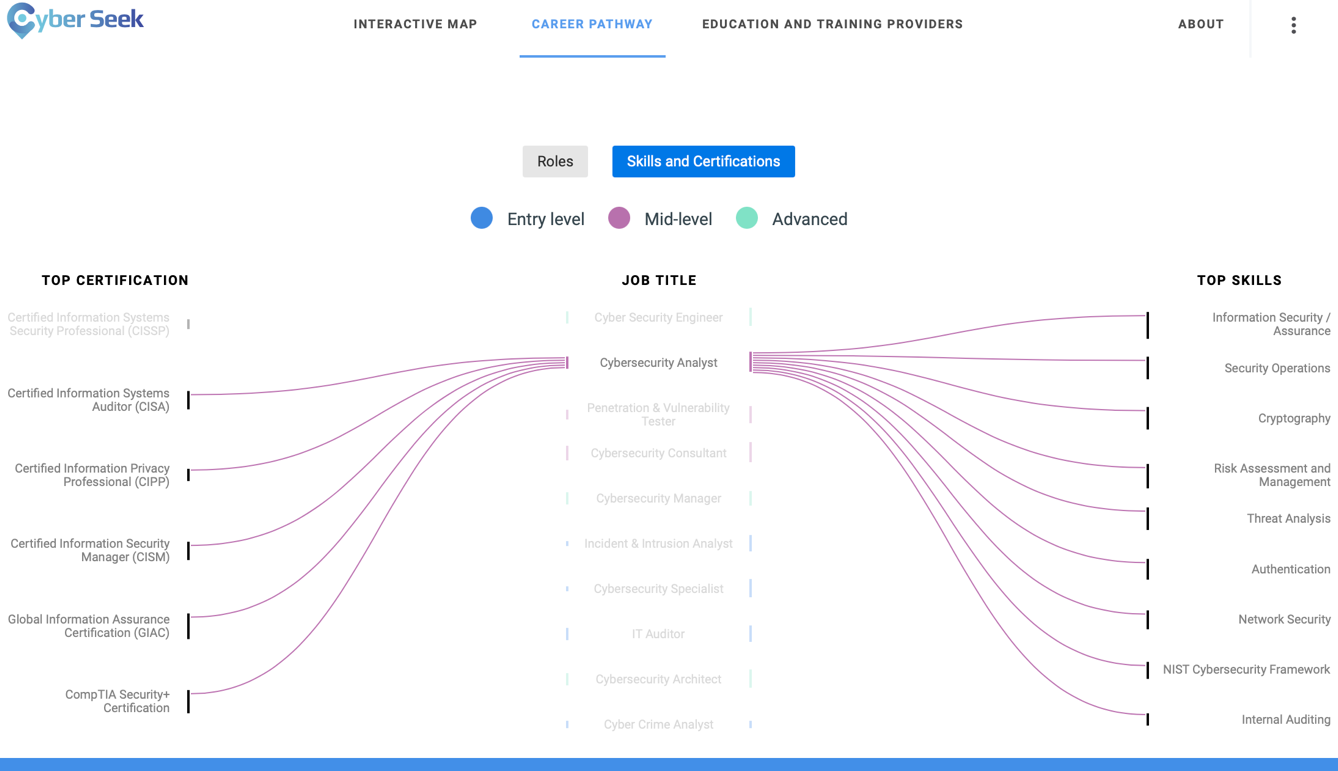
**NICE Framework**

The NICE framework covers every career needed to create a successful cyber staff and more. The SP category covers areas like risk management, system architecture, and system development (NIST, 2017). A cybersecurity architect is an advanced level job that requires certification such as Certified Information Systems Auditor (CISA), Certified Information System Security Professional (CISSP), and other types. They must have skills in the field of network security, NIST Cybersecurity Framework, cryptography, and other advanced skills.



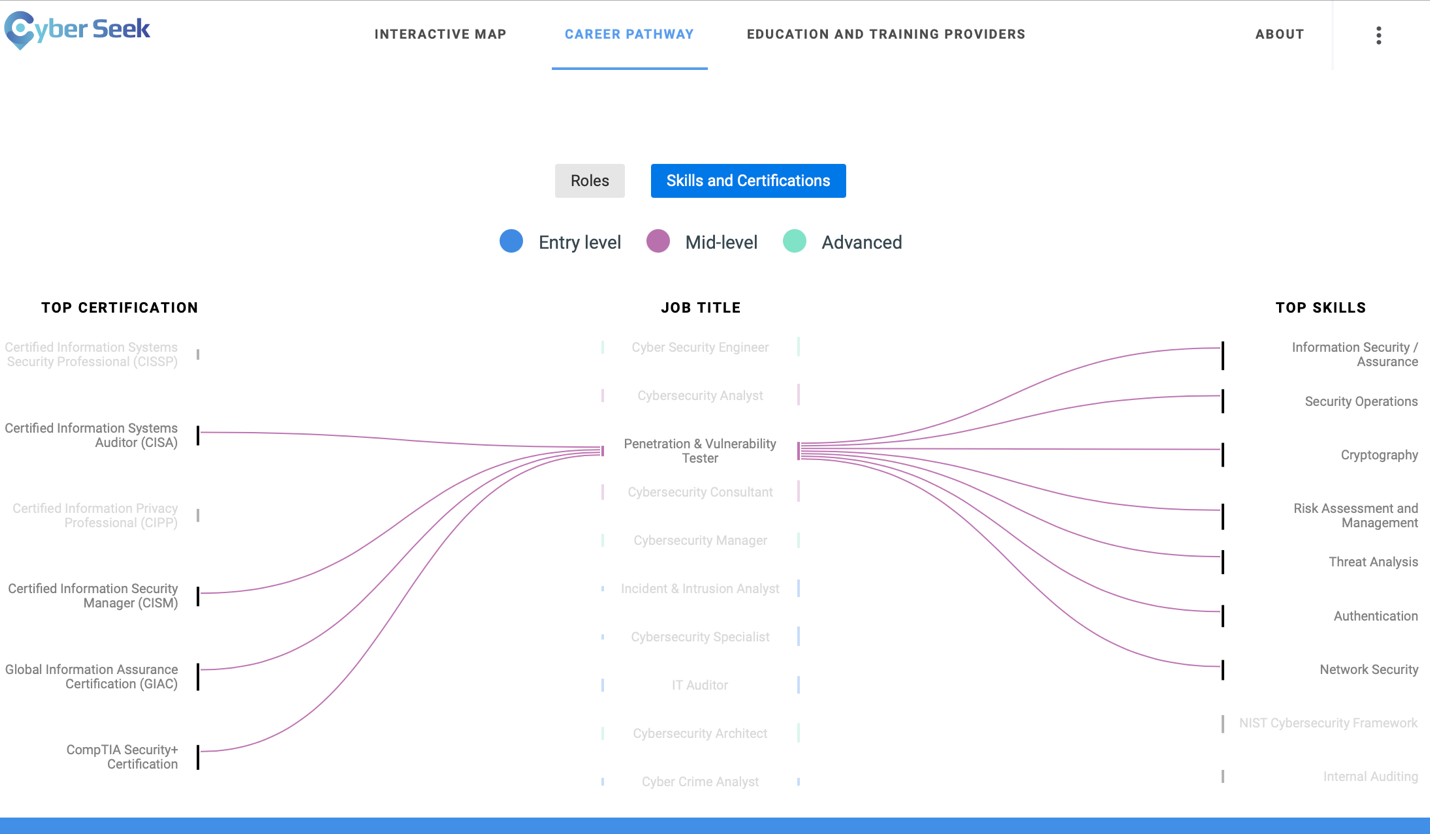
(Cyberseek, 2022)

The OM category expresses job roles such as database administrator, data analyst, and technical support. The OM's sole purpose is to support, administer, and maintain the systems (NIST, 2017). This category can range from entry-level to mid-level, depending on what job role someone is fulfilling. A cybersecurity analyst will be a mid-level position and requires a vast skill set to be successful.

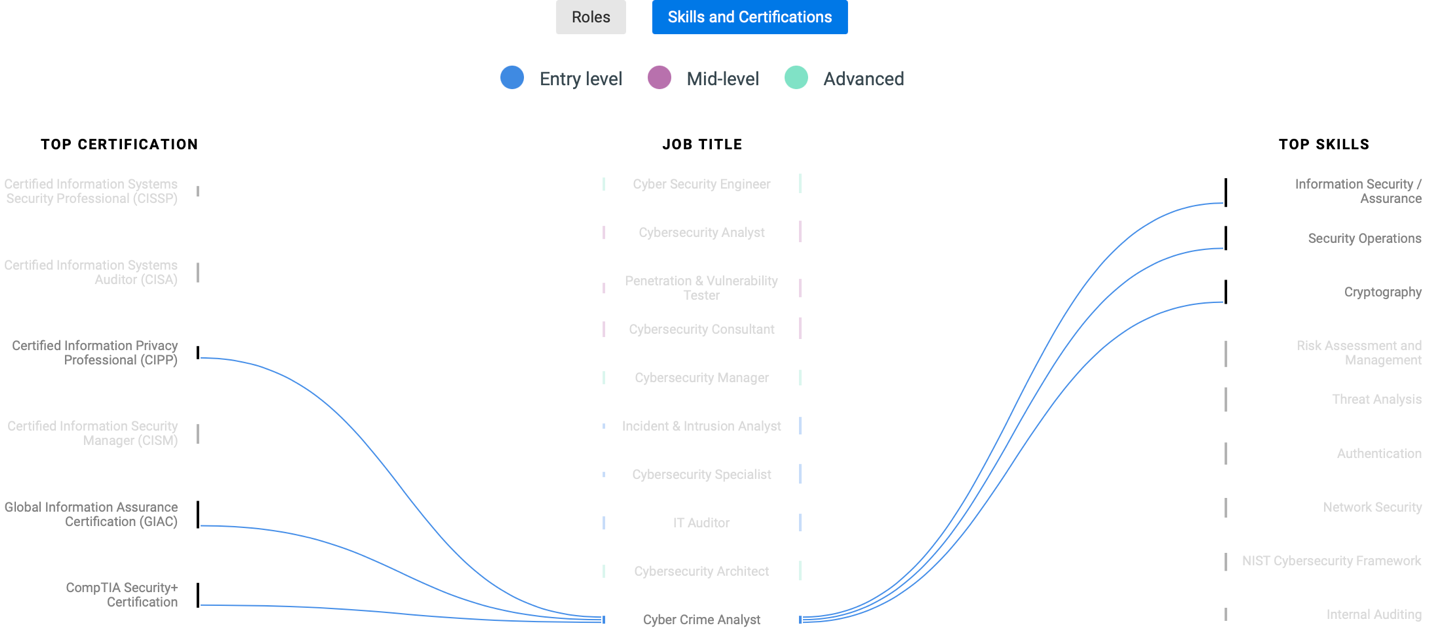


(Cyberseek, 2022)

The OV category provides leadership and management, typically the C suite work roles. Cybersecurity management or executive cyber leadership is an executive-level job, including CISO, Chief Security Officer (CSO), and other executive levels. They have the most experience, skills, and knowledge concerning security for the organization. The PR category identifies, analyzes, and mitigates threats within the system (NIST, 2017). They are an organization’s red or blue hat team and provide the most up-to-date defensive and improvement strategies against threats. A penetration & vulnerability tester is a mid-level career that requires skills such as information security assurance, threat analysis, and network security.



(Cyberseek, 2022)

The AN category reviews and evaluates cybersecurity data and determines if it has a purpose in the intelligence realm. The CO category collects information that may be used to develop intelligence. These two categories correlate and support each other. These job roles include mid-level analysts and planners specializing in exploiting, collecting, diagnosing, and languages (NIST, 2017). Lastly, the IN category investigates crime related to the IT field. This line of duty includes entry-level jobs such as cybercrime investigator and forensics analyst.

(Cyberseek, 2022)

Each category has the sole purpose of meeting all the angles of the cybersecurity industry. Cybersecurity is rapidly growing, and it is projected for information security analysts to have an increase of 35% in jobs by 2031 (BLS, 2022). Fulfilling each category of the NICE framework will develop a prospering team ready to handle any operation.

**Organization’s Mission Statements**

Different organizations require different standards depending on their mission statement. Northrop Grumman, a well-known aerospace company, presents their values as becoming a pioneer with an inventive spirit (Northrop Grumman, 2022). They shape their organization by “defining possible.” Lockheed Martin, another well-known aerospace company, presents their values as solving complex challenges and conducting scientific discovery (Lockheed Martin, 2022). They both, however, require the same qualification, experience, and education when looking for a cybersecurity engineer. The key difference is if an individual's attributes and characteristics meet their mission statements. Northrop Grumman will most likely choose an individual who describes themselves as innovators but Lockheed Martin will choose an individual who describes themselves as a critical explorer.

**Conclusion**

The development of a successful cybersecurity team will take time and effort. Using the NICE framework is a fundamental starting point when debating what job roles to bring on board. Every job role has different levels of education, experience, certification, and skills needed to comply with the duties. Although an individual may meet those requirements, the organization's mission statement will decide if the individual reflects its values.

References

Aiyer, B., Caso, J., Russell, P., & Sorel, M. (2022). *New survey reveals $2 trillion market opportunity for cybersecurity technology and Service Providers*. McKinsey & Company. Retrieved December 4, 2022, from https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers

BLS. (2022). *Information security analysts: Occupational Outlook Handbook*. U.S. Bureau of Labor Statistics. Retrieved December 4, 2022, from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Cyberseek. (2022). *Cybersecurity Career Certifications*. Cyberseek. Retrieved December 4, 2022, from https://www.cyberseek.org/certifications.html

Indeed. (2022). *Guide to Entry-Level Cybersecurity Job Requirements*. Indeed. Retrieved December 4, 2022, from https://www.indeed.com/career-advice/finding-a-job/entry-level-cyber-security-jobs-requirements

Lockheed Martin. (2022). *Who We Are*. Lockheed Martin. Retrieved December 4, 2022, from https://www.lockheedmartin.com/en-us/who-we-are.html

Moore, M. (2022). *How Can I Get an Entry-Level Cybersecurity Job?[Career Guide]*. University of San Diego Online Degrees. Retrieved December 4, 2022, from https://onlinedegrees.sandiego.edu/entry-level-cyber-security-jobs-guide/

NIST. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*. NIST. Retrieved December 4, 2022, from https://www.nist.gov/system/files/documents/2019/11/08/nist.sp\_.800-181.pdf

Northrop Grumman. (2021). *Our Values*. Northrop Grumman. Retrieved December 4, 2022, from https://www.northropgrumman.com/who-we-are/our-values/

Rand, B. (2022). *How To Become a Chief Information Security Officer*. Indeed. Retrieved December 4, 2022, from https://www.indeed.com/career-advice/finding-a-job

Uche, N. (2022). *How to get a job in cybersecurity: Cybersecurity Job Requirements*. Forbes. Retrieved December 4, 2022, from https://www.forbes.com/advisor/education/entry-level-cyber-security-jobs-guide/

Uche, N. (2022). *What is a Typical Cybersecurity Salary?* Forbes. Retrieved December 4, 2022, from https://www.forbes.com/advisor/education/cyber-security-salary-outlook/

Zippia. (n.d.). *Cyber Security Specialist Education Requirements*. Zippier. Retrieved December 4, 2022, from https://www.zippia.com/cyber-security-specialist-jobs/education/