NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

EMPLOYER PERSPECTIVE ON HIRING

FROM THE NICE MODERNIZE TALENT MANAGEMENT WORKING GROUP
NOVEMBER 2022

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

CONTENTS

INTRODUCTION

The objective of this working group project is to examine the employer role in cybersecurity hiring at the early career level. Do employers do enough to create opportunities for those newly entering the field to find suitable work experience? Are job seekers and job providers using the same language and hiring systems to find one another?

This project supports Goal 3 of the NICE Strategic Plan: Modernize the Talent Management Process to Address the Cybersecurity Skills Gaps. In particular, the work addresses:

3.3: *"Align qualification requirements according to proficiency levels to reflect the competencies and capabilities required to perform tasks in the NICE Framework."*

3.4: *"Promote the establishment of more entry-level positions and opportunities that provide avenues for growth and advancement."*

The members of the Modernize Talent Management Working Group created two project teams to collaborate on this effort, one to reflect the Job Seeker perspective, the other to reflect the Employer perspective. This report is for the Employer perspective.

The co-leaders for the Employer perspective group were Peter Meehan and Neferteri Strickland.

UNDERSTANDING THE PROBLEM

Despite the incredible demand for cybersecurity talent, there is debate over how best for someone to enter the field. Few, if any, advertised roles are defined as “entry level”; it’s estimated that fewer than 2% of the roles on CyberSeek (cyberseek.org) are tagged as entry level. Most advertised positions require several years of experience and professional certifications to qualify. Some employers prefer people with the ability to hit the ground running and will pay recruiters fees to “poach” talent, rather than develop someone themselves.

How does someone enter the field from community college or higher education where they are seeking a first professional opportunity? Or transitioning into civilian careers from active military where the candidate may have experience in cybersecurity but need help to translate what they know? For those who want to pivot or retrain for cybersecurity from an unrelated field - what is the best pathway to do that? Which courses, bootcamps, online materials or certifications lead to a job?

Often, applicants are recommended to begin in adjacent positions or “feeder” roles. NICE-funded website, CyberSeek identifies many of these feeder roles, including software development, IT help desk, and network management. And yet, the complexity of job descriptions, of employer requirements makes career pathways very challenging for candidates to navigate. They simply don’t know how to break through all this “gate keeping.”

OPPORTUNITY

The opportunity before the Modernize Talent Management group is to leverage the NICE community in raising awareness of the problem and identifying what needs to be done to change the environment. Employers claim they want to hire "differently" but without an agreed upon strategy it will be difficult for momentum to be built. Therefore, this project must provide simple and focused ideas that any employer can follow. There are two goals: promote more early career entrant hiring and align those new positions to the NICE Framework, including proficiency levels.

This report additionally explores the reasons for apparent resistance from employers to hire junior talent. It then suggests strategies employers can make to ensure new talent can succeed at their organization: to meet hiring criteria; to be trained on the job; to enter into career pathways; to be mentored and retained. It then makes best-practice recommendations on how and why employers could invest in designing, developing, and retaining talent.

The NICE Workforce Framework for Cybersecurity

The NICE Workforce Framework for Cybersecurity (NICE Framework) or NIST SP 800-181 is a crucial reference document for the cybersecurity workforce industry as it defines the work that cybersecurity professionals do by the knowledge and skills required to perform common tasks. These knowledge (k), skill (s) and task (t) statements are organized by 52 work roles within seven categories. Much like the industry of cybersecurity itself, these work roles continue to evolve, and the NICE Framework will be a living document with ongoing public work to ensure it remains relevant. A work role, it should be noted, is not the same as a position description. A single position may include multiple work roles.

Recently (August 2022), a report to Congress included work on the relationship of proficiencies to the NICE Framework; this work should be included in this document so that anyone creating position descriptions that align to the NICE Framework for early career work should be able to leverage it. Employers should utilize the NICE Framework when creating position descriptions and defining career pathways.

DEFINITIONS

Early Career level

There are different interpretations of the term 'entry-level'. And in the industry, some practitioners actively push back: 'Is there really an entry-level position in cybersecurity?' Many would state that other positions help develop and demonstrate certain skills that qualify an individual for cybersecurity work. CyberSeek, the NICE grant-funded website that documents cybersecurity industry supply and demand, shows few open "entry level" defined positions. This would indicate the majority of hiring is not occurring at that level.

Therefore, it may be useful to expand the notion of what entry level work in cybersecurity is. It may be a first position, a career entry point into cybersecurity. For some, that may be a transition from a college degree program; from active duty military; or from an apprenticeship program. It may include a move from a feeder role in an adjacent field such as software development, IT help desk or network management. Therefore, for the purposes of this paper, the guidance here is meant for someone seeking to enter into a cybersecurity career from a number of different starting points. We will consider those individuals to be at the early career level.

(ISC)2 considers entry-level as those "with less than 12 months of experience." It is unclear if that excludes those in the pipeline up to interview and before being hired. CyberSeek considers entry-level as having between 1 to 2 years of experience.

Reskilling

Someone reskilling is currently employed in a different field, such as marketing and needs to go through a job training program to learn cybersecurity job skills. They would benefit from a program like an apprenticeship, where they can skip over general education requirements one might find in a college course and focus on the job-related knowledge requirements. Reskilling programs might also be found in-house at an employer who is able to identify talented individuals and retain them by providing them with a program of education and training that leads to a new job.

Upskilling

Upskilling is a program that enables the employee to continue to grow in their knowledge and skills while on the job, leading them to increased job opportunities with the same employer. This may include educational opportunities via a learning management system (LMS), or the employer may simply reimburse via a tuition credit program. Upskilling may not necessarily be tied to a new job program but be part of ongoing opportunities for continuing knowledge and growth.

MARKET FORCES

Inefficient matching of job candidates to employers

- If it is a low unemployment market, why do so many individuals trained in cybersecurity fail to secure employment in the field? Why aren't employers investing in the development of the hundreds of thousands of graduates from community colleges and universities that can't get jobs or an internship or on the 200,00 veterans who transition from active military duty each year?

- There is a disconnect between employer perceptions of the time and expense for new hires to become productive and what research indicates. (ISC)2 research shows that it takes under 1 year and less than $1,000 in training costs for a new hire to work independently.

- Increased hiring in sectors like healthcare, retail, and manufacturing further fragment the marketplace, which should make employers more flexible with candidates. Rather, the market seems to increase reliance on recruiting firms and increased salaries to seek seasoned talent.

Burnout, low morale, and retention issues are endemic

- An (ISC)2 Workforce study noted concern around reasons that cybersecurity professionals leave a job. Although many who left their jobs cited higher pay and more growth opportunities, the next major reasons for leaving a job were: negative culture, burnout, and poor work/life balance.

- The study also notes that staff retention continues to be an issue in cybersecurity. As such, there is turnover in the workforce, supporting the need to develop a robust pipeline of cybersecurity professionals.

EXECUTIVE SUMMARY

We need a moon-shot mission mentality by employers to address the cybersecurity talent gap for the long run

Recommendations

- Employers need to build their own talent pipelines, with investment at early career stages
- Employers need to adopt the NICE Framework across their entire ecosystem
- Employers need to engage their human resources and talent acquisitions teams as full partners in the cybersecurity workforce solution:
  - Creating realistic position descriptions that do not list unnecessary required qualifications
  - Developing talent management systems and career pathways aligned to the NICE Framework
  - Leveraging artificial intelligence software and learning and employment records (LER) to identify talent and to support employee development

Strategy 1: Employers need to build their own talent pipeline, with investment at early career stages

> "A large organization should aspire to have as much as 50% of their cybersecurity team at entry level"
> Alan Berry, CISO, during a July 2022 NICE Community Coordinating Council meeting

It is essential to bring all organization stakeholders onto the same page: from the C-suite, human resources, learning managers and the cybersecurity team. The hiring manager needs to help everyone understand the severity of the issue - using marketplace data to underscore why it is hard to rely on mature talent to solve hiring needs and why it is time to invest in a new model for ensuring a long term and stable talent pool. Additionally, there are opportunities to achieve diversity, equity, and inclusion gains if the organization considers programs like apprenticeships and military-to-civilian job training programs.

Employers should also work with internal staff to create programs that enable current team members to be assessed for their interest and aptitude for cybersecurity. The organization can set up programs to retrain and reskill them for future positions in cybersecurity.

This means that employers must work with the educational and job training community to clearly define the knowledge and skills they require for their jobs. They should also be working with their internal stakeholders to define work and work roles required that can be performed by those just entering the workforce; by those who are retraining from adjacent technical positions such as information technology; and by those who are reskilling and upskilling to enter cybersecurity careers. This will require detailed knowledge of the work they perform - none of this is casual effort but is an overhaul of the approach taken to fill one expensive mid-career professional role at a time.

Employers should work to define their positions using available standards such as the NICE Framework to ensure that candidates can self-identify what positions they can qualify for. Using the NICE Framework, one can access courses at a community college, a university, or a certification provider and recognize what knowledge one might acquire. Employers are increasingly able to see the quality of education available at community colleges and the National Security Agency (NSA) Centers of Academic Excellence (CAE)-designated colleges and universities. Competitions are often able to help a candidate demonstrate knowledge with practical skills-based labs to the satisfaction of the employer. This can only work, however, if the candidate, educator, trainer, and employer are all sharing the same playbook to establish what those standards are. This is the purpose of the NICE Framework. It is long past time for employers to utilize this reference work.

Other ways to bring in new talent to an organization:

Apprenticeships - Employers can also adopt well-recognized on-the-job training methods such as Registered Apprenticeship programs to develop new talent. There are hundreds of such programs in cybersecurity and information technology fields today. These are highly successful methods for discovering and developing new talent, often individuals from under-served populations who offer diverse perspectives for the company. Apprenticeships deliver a positive return-on-investment and have proven to be an effective talent pipeline to deliver custom-trained employees with in-demand skill sets. More information can be found at **apprenticeship.gov.**

Internships - an internship is a less formal, short-term program with a high school, community college, or university student for hourly pay or for credit at their institution. Typically, they are assigned a mentor or supervisor and provided with project work that is meant to introduce them to the field of their interest. There is no expectation of a full time job at the completion of the time period.

Co-op programs - these are more formal programs of cooperative education and work experience. Universities like Drexel and Northeastern were pioneers in this sort of educational method. The student learner is balancing periods of classroom time with time on the job. A co-op position may be both paid and for credit at the institution the student is attending. They are for a short, defined period of time. There is no commitment to hire the student upon completion of the program.

Military-to-civilian career transition programs such as Skillbridge - this is a Department of Defense program allowing pre-transition (last 180 days of service) military personnel to enroll in apprenticeship-style work experience with civilian employers. They are still employees of the military, but they gain civilian work experience, easing the transition to civilian life and helping to create a resume while gaining experience in the private sector. The military continues to pay the salary of the active duty military member while they report for work experience at the civilian job site.

Other examples include return to work programs for women and displaced workers; job training programs for underserved populations such as YearUp and NPower.

Strategy 2: Employers need to adopt the NICE Framework across their entire ecosystem

All stakeholders should adopt the NICE Framework: to create a position description, to recruit for new staff, to set interview guides, to hire and train. The NICE Framework should be used to identify gaps in staffing and to create career pathways and identify opportunities to help employees build their careers. As the NICE Framework is evolving to include competency areas, it is expected that a mature organization will continue to revisit the NICE Framework on a regular basis and update relevant materials to ensure compatibility. Additionally, if they are using systems that also leverage the NICE Framework, such as Learning Management Systems or Learning and Employment Records, they will need to ensure that their vendors align to the same standards and current version as their organization.

An advantage of adopting the NICE Framework is that organizations will be primed to evolve to a skills-based approach to hiring. This means gaining a wider talent pool and greater diversity. It means that candidates who were previously getting screened out because they lacked a prestigious degree or credential can now be identified. It means that self-taught individuals get equal access to positions as those who could afford a four-year degree program. This method requires employers to invest in technology or services to help them first to identify which skills are necessary to succeed and then to validate the candidate's skill set.

Strategy 3. Employers need to engage their human resources and talent acquisitions teams as full partners in the cybersecurity workforce solution

- Creating realistic position descriptions that do not list unnecessary required qualifications
- Developing talent management systems and career pathways aligned to the NICE Framework and Competencies
- Leveraging artificial intelligence software and learning and employment records (LER) to identify talent and to support employee development

The human resources (HR) and talent acquisition teams have a significant role to play and must be brought into the stakeholder community for the cybersecurity workforce. This includes increasing HR and Talent Acquisition professionals' representation with the NICE program and attending NICE conferences. NICE is currently developing training materials in partnership with the SANS Institute and the Society for Human Resource Management (SHRM) to help support this concept.

This is further supported by recent research mentioned earlier in this report from the International Information System Security Certification Consortium (ISC2). Their Cybersecurity Hiring Managers Guide 2022, states:

- Finding and nurturing newcomers to the field requires a shift in recruiting tactics and an investment in training to enable new hires to learn and grow.
- 37% of hiring managers said entry- and junior-level hires are ready to handle assignments independently within six months or less on the job.
- For this study, entry-level team members are defined as staff with less than one year of experience. In contrast, junior-level practitioners have one to three years of experience.

Creating realistic position descriptions is a concept mentioned in other industry research reports. In the 2018 Aspen Cybersecurity report, "Principles for Growing and Sustaining the Nation's Cybersecurity Workforce," the authors set out recommendations that included dropping onerous requirements that effectively block many from applying for cybersecurity work. Such requirements might include college degrees, years of experience, certifications. Employers should consider whether everything they list as "must have" on their position descriptions could be altered to become "may have" or removed.

The language used in position descriptions should be straightforward; reflecting common terminology and not company speak or military language. Avoid gendered language that might prevent women or female-identifying candidates from applying. There are text-based tools to assist human resources in evaluating content to spot inequities in language and recommend ways to improve it.

Offensive Security recently authored a guide for writing entry level position descriptions that includes templates for two positions, Secure Operations Center (SOC) Analyst and Penetration Tester. The document includes sample text with simple language an employer can customize for their needs. The author encourages employers to write job postings in a way that applicants can imagine themselves in that position, to highlight training, mentoring and career development the employer offers and other key tips.

As noted in a TechRepublic article, "soft" skills are also critical for cybersecurity roles. Among the skills mentioned in the article are attention to detail, risk awareness, effective communication, and problem-solving capability. The article further notes the importance of clear and effective communication for any cybersecurity role.

The NICE Framework knowledge and skill statements are ideal for adopting in the creation of position descriptions. Human resources and talent acquisition professionals may not be aware of their utility for this purpose. And the NICE Framework proficiency work mentioned earlier, is suitable to leverage in creating junior or career-entry positions, describing mid-career positions and identifying pathways to senior positions in the same career pathway. Ideally, all of these efforts should be part of a work project that includes setting clear and explicit requirements and expectations for each job on a pathway. These expectations should also be part of a learning plan so that employees who are working on an upward career trajectory can identify courses and programs to take that will gain them needed skills and knowledge for their next career step.

Skills-based hiring is the logical result of adopting the NICE Framework. In this approach, the employer emphasizes the achievements of the individual gained through the combination of work experience and learning, whether acquired in the classroom or on the job. It is the recommendation of The National Governors Association, Skills-Driven State Community of Practice, and the Business Roundtable, among other leading organizations.

Leveraging Artificial Intelligence software and Learning and Employment Records to identify talent and to support employee development

The NICE Modernize Talent Management Charter included investigating artificial intelligence tools and technology to improve talent acquisition. The traditional talent acquisition search engines do not have the granularity of keyword search or taxonomy suitable for risk and cybersecurity roles and functions. Keyword search, however, is not the only method of finding talent. For example, there is an increasing number of aptitude, attitude, and suitability assessment tools.

Several Federal agencies and private sector firms have adopted the CyberStronger CYBRScore skills assessment methodology to assess and identify people with the potential to enter cybersecurity careers along NICE Framework-aligned pathways. This helps them find good-fit candidates and identify the training required to support them in meeting requirements. These assessments may help employers decide on which talent to invest in before hiring or transferring into cybersecurity positions.

Humanico, an Australian Technology innovator in the HR Tech vertical, has built a digital interactive human map to enable companies to understand and optimize their people based on a number of emotional and psychographic attributes, mostly self-reported. AustCyber is partnering with Humanico and its platform to assess and improve the capability of the Australian cybersecurity workforce. The platform leverages the CliftonStrengths® methodology, globally validated and underpinned by science with over 26 million data points to understand how people think, feel, and behave naturally. This, combined with other Humanico services, reveals how employees feel about their work, providing deep insights into the population's capability. Insights enable organizations to map their business strategy back to people-capability. Humanico and AustCyber are helping address the critical skills shortage by supplementing key additional data metrics and providing a more holistic approach to the problem space.

Learning and Employment Record (LER) aka the Digital Wallet

The NICE Community has led several webinars and discussions about the emergence of the learning and employment record (LER) or digital wallet, an effort to help the employee track their acquisition of knowledge and skills across their career, from workplace to workplace as well as at all formal learning experiences. Attend a conference or lecture or learn something on the job - every activity leads to an earned digital credential that is stored in a blockchain secured wallet that follows you electronically.

T3 Innovation Network, US Chamber of Commerce, American Workforce Policy Advisory Board, and the National Governors Associations are promoting the use of interoperable LERs. Most LERs are being developed in academia to transfer transcripts between institutions at this stage. However, iQ4 Corporation collaborated with the National Student Clearinghouse (NSC) and IBM to build a version focused on cybersecurity.

It was first demonstrated to the White House Administration in September 2020. Since then, the taxonomy capabilities have been extended to address IT roles and healthcare with more disciplines and sectors to follow. Western Governors University (150,000 users) and University of Cincinnati (>1,000 users),

and the Idaho Achievement Wallet program under the Governor, to name a few, have adopted the LER. All 1,700 Veterans, spouses, dependents, and DEI community people taking the DOL-funded work-based learning course at Clark University will have their LER free for life.

Some of the additional benefits of adopting LERs are their capabilities to: leverage the machine language and artificial intelligence to turn ingested documentation, such as academic transcripts, military transcripts, certificated evidence, white papers, and project documentation, into a skills-based taxonomy.

Employers should ensure that their environment supports the emerging LER community and ensure that their employees' experiences are contributing to their LER. This may require them to align the wallet owner to their job or profile via the NICE Framework. This might identify employee skills gaps; enabling learning opportunities to be identified and courses in the employer's supported learning management system to be linked to.

The employer can further support the effort by creating a digital portfolio by ensuring that documents, badges, certificates, videos, photos are uploaded to the system. Enable the owner to confirm and document their competencies for each relevant KS statement with evidence statements. Link to career pathway tools with job descriptions and help the employee identify missing skills or fit to future or adjacent roles.

Thinking towards the future - as these wallets continue to be adopted broadly and evolve, the marketplace for skills becomes more equitable. Each wallet owner can describe themselves in a skill-based manner. Wallet data can be shared, so that employers can more efficiently identify talent around the world, sourcing best-fit candidates, reducing the reliance on resumés and cover letters.

Thinking beyond these concepts

Regional Employment Stakeholder Groups - Employers need to build local relationships with education and training providers in their communities that prepare entry level talent. As part of building their pipeline, they can reduce reliance on recruiting services and out-of-state career fairs to focus on those in their own community. NICE funded a series of popular and successful regional grant programs known as Regional Alliances and MultiStakeholder Partnerships to Stimulate (RAMPS) in 2016; should Congress reinstate and support their funding again, these will be a good mechanism for re-establishing and expanding this program in additional regions. The project team and members of the Modernize Talent Management working group recommend that employers do not wait for these grants. Rather, they can make these connections themselves by engaging directly with their local workforce boards, community colleges, universities, job training organizations, etc.

Sector-specific hiring - The current NICE Framework taxonomy describes 52 work roles. For sectors with hybrid work requirements (such as health care with regulatory requirements), a cybersecurity professional may need training in clinical environments and technical knowledge.

Therefore, those who understand and appreciate the NICE Framework taxonomy can use it to shape the role profiles and job families they need at any time. For example, CommunityHealth IT (CommHIT), a 501(c)(6) at the Kennedy Space Center, created hybrid roles for telehealth and cybersecurity first responder operatives using DOL H1-B program grants, particularly for businesses in rural and underserved settings in Florida.

More people residing in geographically remote areas are connected to digital health services, such as medical remote monitoring devices, and become networked to hospitals and tertiary care located in more urban areas. It would be unaffordable to staff cybersecurity personnel in those rural locations near the patient, therefore training workers for hybrid roles involving both cybersecurity and telemedicine is a foundation for improved coverage and protection. This initiative is expanding to a national program.

Technology-specific hiring - A holistic picture of cybersecurity risk considers both Information Technology and Industrial Control Systems / Operational Technology/ (ICS/OT). There are work roles emerging that are not only sector-specific but require a combination of cybersecurity and industrial control skills. This is seen in the energy sector where new OT/cybersecurity apprenticeship programs from EnergySec have just been created in partnership with Everett Community College.

While technology needs people to deploy and operate, cybersecurity – and risk mitigation – is not just about technologies and technical competencies. Burgeoning pressures from regulators across multiple jurisdictions are driving demands for interaction between the board, business lines, IT/CISO office, and the regulators. Governance Risk and Compliance (GRC) primarily has research, analysis, communication, and reporting competencies. GRC roles often do not require technical skills or expertise but require the ability to articulate technical content. GRC roles are currently in high demand and could potentially provide paths for entry-level candidates.

There isn't just one answer and no shortcuts either. The solution requires a cultural shift and an economical way of developing talent. Short-term strategies that avoid designing, developing, and building the talent an employer needs will only worsen the problem. A Return-on-Investment (ROI) model is required to show employers that investing in building future talent and hiring them is viable.

Future Research Opportunities

There are many potential avenues for research to support early career hiring. The team recommends conducting research into the following topics:

- What is the **return-on-investment** for training current employees for career progression to someday fill senior level roles? Often cybersecurity training programs can be expensive for an organization. In addition, organizations fear employees will leave after getting trained. However, retaining employees who have no path for progression has proven difficult. Research would have to demonstrate the cost benefit of training current talent with a clear path to progress into senior roles.

- Which **less technical work roles** are ideal career entry points for cybersecurity in addition to those most often cited [Secure Operations Center (SOC) analyst, cybersecurity support specialist, IT help desk, etc.]? For example, which are well suited for career switchers lacking technical skills but with legal or government experience: i.e., governance, risk, compliance, policy, vendor management and cybersecurity training and awareness roles.

SUMMARY

The time has passed for cybersecurity hiring organizations to establish robust talent systems that include opportunities for non-traditional sources of talent. Every cybersecurity employer can dramatically increase the number of their early career opportunities. This isn't a call for organizational chaos. This must be part of a structured plan for creating a program of mentoring and opportunities for on-the-job learning for people at every level in the cybersecurity team. No one should look at the early career cohort with envy that they receive the training opportunities. Include those learning and reskill/upskill opportunities at every stage of the career pathway and as part of an overall managed learning and workforce program.

It is possible for the employer to reduce their time to hire statistics. To improve their cybersecurity team's morale. To even improve retention figures and end burn out. It's in the employer's own interest to make this shift and do things differently.

In summary,

- Employers need to build their own talent pipelines, with investment at early career stages
- Employers need to adopt the NICE Framework across their entire ecosystem
- Employers need to engage their human resources and talent acquisitions teams as full partners in the cybersecurity workforce solution:
  - Creating realistic position descriptions that do not list unnecessary required qualifications
  - Developing talent management systems and career pathways aligned to the NICE Framework and Competencies
  - Leveraging artificial intelligence software and learning and employment records (LER) to identify talent and to support employee development

NICE

NATIONAL INITIATIVE FOR
CYBERSECURITY EDUCATION