Cybersecurity Careers of the Future

December 2018

CISA
CYBER+INFRASTRUCTURE

Cybersecurity Careers of the Future

Table of Contents

I. Introduction

This white paper sponsored by the Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security, and authored by the Software Engineering Institute at Carnegie Mellon, is the summary results from exploration into the state of cybersecurity job roles essential to protect and defend in cyberspace. The desired outcome is to identify the skills and abilities needed for future cyber workforce, determine which are critical, and leverage the findings to better scope training and outreach initiatives.

Numerous reports highlight the growing need for cybersecurity talent. Some estimates even forecast a shortage of nearly three million qualified professionals over the next two years.[1] To prepare for this challenge it is necessary to train future talent in this field. However, the breadth of cybersecurity is so wide that it is difficult to know exactly what to include within a curriculum. It is necessary to take a holistic review of a diverse set of cybersecurity reports, studies, and resources to better pinpoint these needs. Analyzing workforce surveys, threat reports, service offerings, open job postings, applicable regulations, and emerging technologies will help identify the needed Knowledge, Skills, and Abilities (KSAs). Using the NICE Cybersecurity Workforce Framework (NICE Framework), we can then determine Work Roles and generate a list of cybersecurity jobs needed to close the workforce gap.

Key findings from this analysis conducted in December 2018 are:

- Traditional Information Technology (IT) roles of System Administrator and Network Operations Specialist are critical Work Roles in the cyber fight. They are often required to identify, configure, and implement security solutions to meet regulation and compliance standards, in addition to applying other best practices.
- Secure software development practices must be integrated throughout the entire Software Development Life Cycle (SDLC). This requires cybersecurity professionals from numerous NICE Framework Specialty Areas to improve coding skills, and Software Developers to enhance secure coding techniques.
- Emerging and evolutionary technologies like Cloud Computing, Internet of Things (IoT), Artificial Intelligence, and Machine Learning create new capabilities. However, they also broaden an adversary's cyber attack surface. In addition to implementing software development procedures, it is paramount to continually audit applications and systems for new vulnerabilities that may be unintentionally introduced.
- Government and industry regulations will drive baseline cybersecurity controls and processes. Managers and Assessors will play critical roles in implementing solutions and validating compliance.
- Greater adoption of NICE Framework throughout government and industry is necessary to create a standard cybersecurity lexicon for employers, educators, and cybersecurity professionals.

- High demand NICE Framework Work Roles are expected to include:
  - Information Systems Security Manager (OV-MGT-001)
  - Information Systems Security Developer (SP-SYS-001)
  - Systems Developer (SP-SYS-002)
  - Software Developer (SP-DEV-001)
  - Vulnerability Assessment Analyst (PR-VAM-001)
  - Security Control Assessor (SP-RSK-002)
  - Cyber Operator (CO-OPS-001)
  - System Administrator (OM-ADM-001)
  - Network Operations Specialist (OM-NET-001)
  - Research & Development Specialist (SP-TRD-001)

II. Current Cybersecurity Workforce

Several resources are commonly cited when discussing the demand for cybersecurity professionals. One of the most referenced is the Information Systems Security Certification Consortium (ISC)² Global Cybersecurity Workforce Study, known before 2018 as the Global Information Security Workforce Study. Their research attempts to capture the current state of the cybersecurity community, along with its top challenges and concerns. (ISC)² was founded in 1989 and consists of more than 138,000 certified members. [2] Their most well-known certification is the Certified Information Systems Security Professional (CISSP). The size of the (ISC)² community, and the success of their programs and research studies, provide us with a good baseline for understanding the current cybersecurity workforce.

The key statistic frequently referenced in articles and reports since the release of the 2018 Global Cybersecurity Study is the estimated global shortage of nearly 2.93 million cybersecurity professionals by 2022.[3] This is an increase of over one million positions from the 2017 estimate, which in turn was a 20% increase from the 2015 forecast. With tens of thousands of respondents participating in these surveys, it is clear there is a need for more cybersecurity talent. What is not clear are the exact skillsets and competencies required for those jobs. We need to take a closer look at each study to identify trends, gap areas, and additional takeaways.

Information security workforce predictions within the surveys from 2004 to 2013 were forecasting the total number of future cyber positions. By our calculations, these generally fell short of the estimates by an average of 18%. This was specifically addressed in the 2015 Survey as the shortfall was attributed to a lack of qualified professionals being available, as opposed to a miscalculated need or the existence of fewer positions. Since 2015, a new methodology has been used to identify the potential cybersecurity workforce gap based on the delta between the supply and demand for this talent.

The (ISC)² Global studies requested a Job Title from their participants. Considering all of the surveys from 2004-2018, the top cybersecurity titles were:

- Security Consultant
- Security Analyst
- Security Systems Engineer
- Security Manager
- Network/Systems administrator
- IT Director/Manger
- Programmer
- Security Auditor

Some related observations include the separation of Security Analyst and Security Engineer beginning in 2011. We also see representation from traditional IT roles throughout the 14 years of data collection. It is often the responsibility of these positions to implement security solutions and best practices, although job titles are not directly tied to cybersecurity.

One of the biggest challenges in analyzing the (ISC)² Global studies is correlating their results over 14 years of evolving survey questions. In some years we have technology initiatives identified, like deploying Wireless or Identity and Access solutions. In others we have training needs listed. In a few others we have specific skill gaps detailed. There were items such as Cloud security referenced in several reports as either a top risk, training area, deployment project, or threat vector.

The following list presents the top cybersecurity areas of focus as extrapolated from the 2004, 2005, 2008, 2011, 2013, 2015, 2017, and 2018 (ISC)² Global Information Security (Cybersecurity) Workforce Studies. Additional weight is placed on the areas of future demand, which were highlighted in 2018:

- Business Continuity and Disaster Recovery (BC/DR)
- Governance, Risk, and Compliance (GRC), including Policy management and auditing tools
- Security Analysis
- Security Engineering
- Security Management
- Security Administration
- Software Development, including the integration of security testing within the SDLC
- Incident Detection and Response

- Network Monitoring, including Security Information and Event Management (SIEM)
- Digital Forensics
- Intrusion Detection/Prevention Systems
- Vulnerability Assessment and Management, including penetration testing
- Cloud Security
- Threat Intelligence Analysis
- Mobile Device Security

There are several other key takeaways from the (ISC)² Global Cybersecurity studies that will help shape the cybersecurity workforce of the future.

- The cybersecurity workforce will be driven by government regulations, new technologies (e.g., mobile, Cloud), and cybersecurity threats.
- Organizations are leveraging security service providers to augment internal security staff or to fill skills gaps.
- 22% of 2011 information security professionals reported some involvement with software development, either with design, specifying requirements, testing, solutions integration, or coding.
- Application security scanning needs to be included within the software development life cycle.
- In 2015, Security Analyst was the most in-demand position with 46% of respondents identifying staffing deficiencies in that area.
- 30% of the 14,000 respondents in 2015 estimate an increased use of managed and professional security service providers, with 49% citing their lack of in-house skills in areas like threat intelligence, forensics, risk management, and compliance.

(ISC)², the Center for Cyber Safety and Education, Booz Allen Hamilton, Alta Associates, and Frost & Sullivan used the results from the 2017 Global Information Security Workforce Study to produce a special report analyzing over 2,600 responses from the U.S Federal Government, including military and non-military professionals.[4] Within this report, (ISC)² members were asked to describe their agency's adoption of the NICE Framework. 30% of respondents claimed their organization had at least partially adopted the framework.

The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework is a national resource that categorizes and describes cybersecurity work. Written collaboratively by the Department of Homeland Security (DHS), the Department of Defense (DOD), and NIST, the NICE Framework consists of seven Categories that provide a high-level grouping of cybersecurity functions. Within the categories are 33 Specialty Areas, which encompass 52 detailed Work Roles.[5]

The NICE Framework is provided as NIST Special Publication 800-181.[6] Its intent is to provide organizations with a common and consistent lexicon for defining cybersecurity activities. It can also be used to identify, develop, and recruit talent, thereby decreasing the cybersecurity employment gap.

Adoption of the NICE Framework is already underway. The Federal Cybersecurity Workforce Assessment Act of 2015 required the Office of Personnel Management (OPM), in coordination with NIST, to develop a coding structure for federal civilian cybersecurity positions. In accordance with this requirement, OPM, NIST, DHS, and Office of the Director of National Intelligence (ODNI) leveraged the NICE Framework to create the necessary guidance for assigning new codes to IT and cybersecurity functions.[7] The DOD Cyber Workforce Framework (DCWF) also leverages the NICE Framework along with its Joint Cyberspace Training and Certification Standards (JCT&CS) to define cyber roles and responsibilities within the military.[8] Internationally, the NICE Framework is being used for initiatives like Cyber New Brunswick (CyberNB[9]) in Canada and AustCyber[10] in Australia. With clear acceptance throughout the world, the NICE Framework is demonstrating its value to the cybersecurity community. Therefore, it will be used throughout the remainder of the report to help identify specific career needs based on the analysis of cyber threats, emerging technologies, managed security services, applicable regulation changes, and by reviewing the available cybersecurity job postings on several employment web sites.

III. Job Board Analysis

The U.S. Department of Labor's Bureau of Labor Statistics projects a higher than average growth rate (28%) for Information Security Analyst jobs.[11] In general, that is great news for cybersecurity professionals, but there is still a slight problem. The tasks performed by an Information Security Analyst may differ from company to company. There is no standard set of KSAs defined for an Information Security Analyst that are used consistently. Even a direct mapping to the NICE Framework does not exist. Perhaps this job is similar to a Systems Security Analyst (OM-ANA-001) or a Cyber Defense Analyst (PR-CDA-001). Or, there may be another half dozen roles within the NICE Framework that it might map closely to.

Cyberseek[12] is an initiative from Burningglass, CompTIA, and NIST. This resource does a great job of mapping job data to the NICE Framework. It shows the total number of online job listings for cybersecurity-related positions, along with an estimated number of workers in specific roles during that data collection timeframe (September 2017 – August 2018). Salary data, common job titles, requested certifications, and top skills are also available. In addition to reviewing this general information on NICE Framework positions, we wanted to go through the user experience of looking for a cybersecurity job.

Many cybersecurity professionals will start their job search by simply browsing the Internet. We replicated this process by automating keyword searches on several popular employment sites. Although the results depend upon the search capabilities of each site, we are still able to use the resulting quantities as a valuable metric for further analysis. All NICE Framework Work Roles

and Specialty Areas were queried on Glassdoor, Indeed, Monster, LinkedIn, Dice, SimplyHired, and USAJobs.gov.[13]

To do this analysis it was necessary to establish a method that consistently measured results from sites having a high disparity in available positions. For example “Program Manager” had about 77,000 results on GlassDoor.com and over 422,000 listings on Indeed.com. It would NOT be fair to say “Program Manager” positions are needed more on GlassDoor, or less on Indeed. Instead of using counts, query results were represented as a percentile of total available positions. Using this method we see that 7% of available 2.2M postings on Glassdoor are returned when searching “Program Manager” along with 10% of Indeed’s 4.2M jobs. When averaged together we have a value of 8.5% that represents the in-demand rating for this Work Role. These average percentiles are then compared, with the highest ratios representing the most sought after jobs. The Top 10 Specialty Areas and Work Roles are displayed in

Figures 1 and 2 respectively. Additional findings include:

- "Information Security" is still more widely used than "Cybersecurity" or "Cyber Security"
  (Figure 3).
- Based on USAJobs.gov results, the Federal government has a higher demand for management related positions versus technical roles.
  - 19 of the 52 Work Role searches on USAJobs.gov displayed 0 openings
- Within the Top 10 Work Roles:
  - 3 were software development/programing related
  - 6 were management focused
- System Administrators did not make the aggregated Top 10, but that Work Role was in the Top 10 on 6 of the 7 queried job boards.
- Within the Top 10 Specialty Areas:
  - 2 of Top 4 Specialty Areas are heavily dependent on software development/programming
  - 6 of Top 10 Specialty Areas significantly benefit from coding KSAs

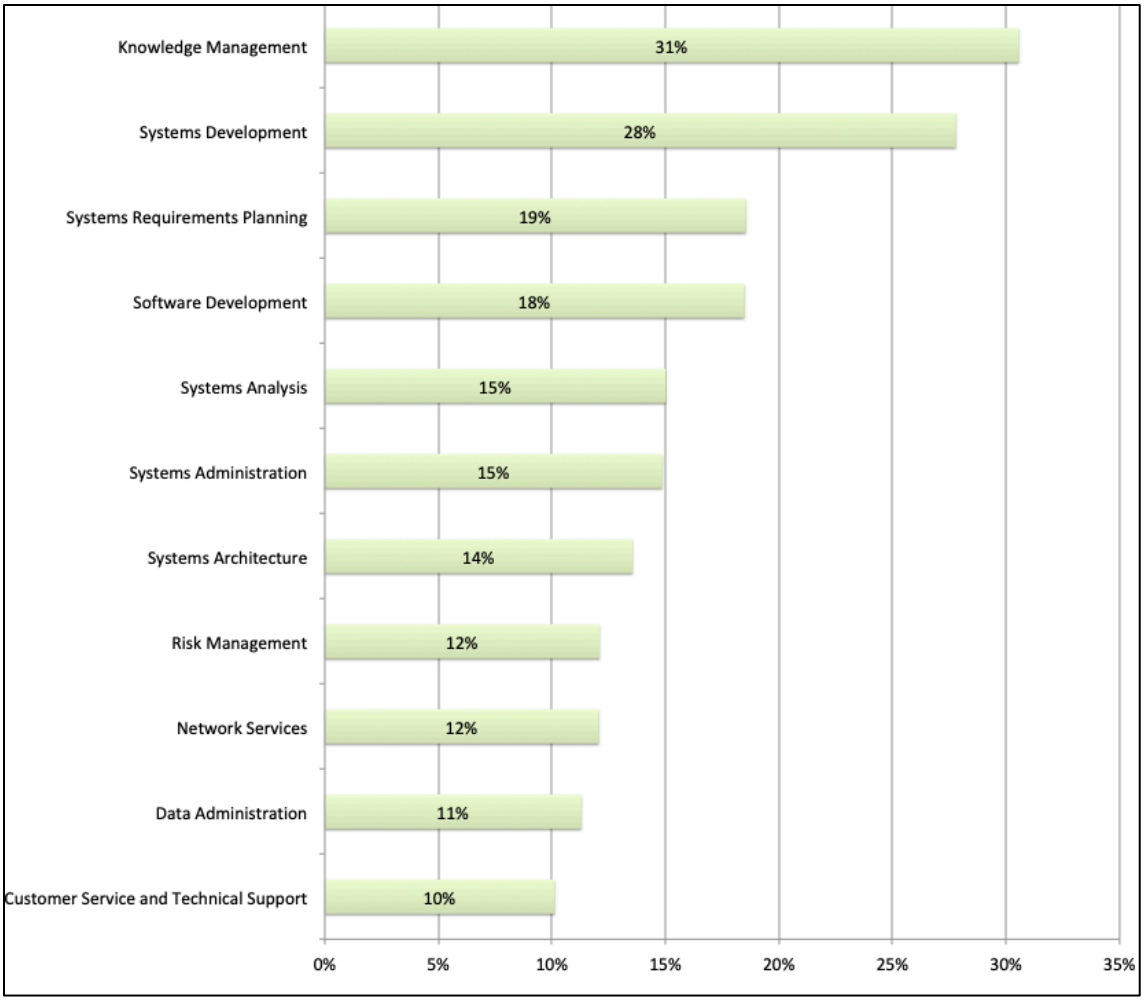

Figure 1: Top 10 Specialty Areas listed on job placement boards (November 2018)

Figure 2: Top 25 Work Roles listed on job placement boards (November 2018)

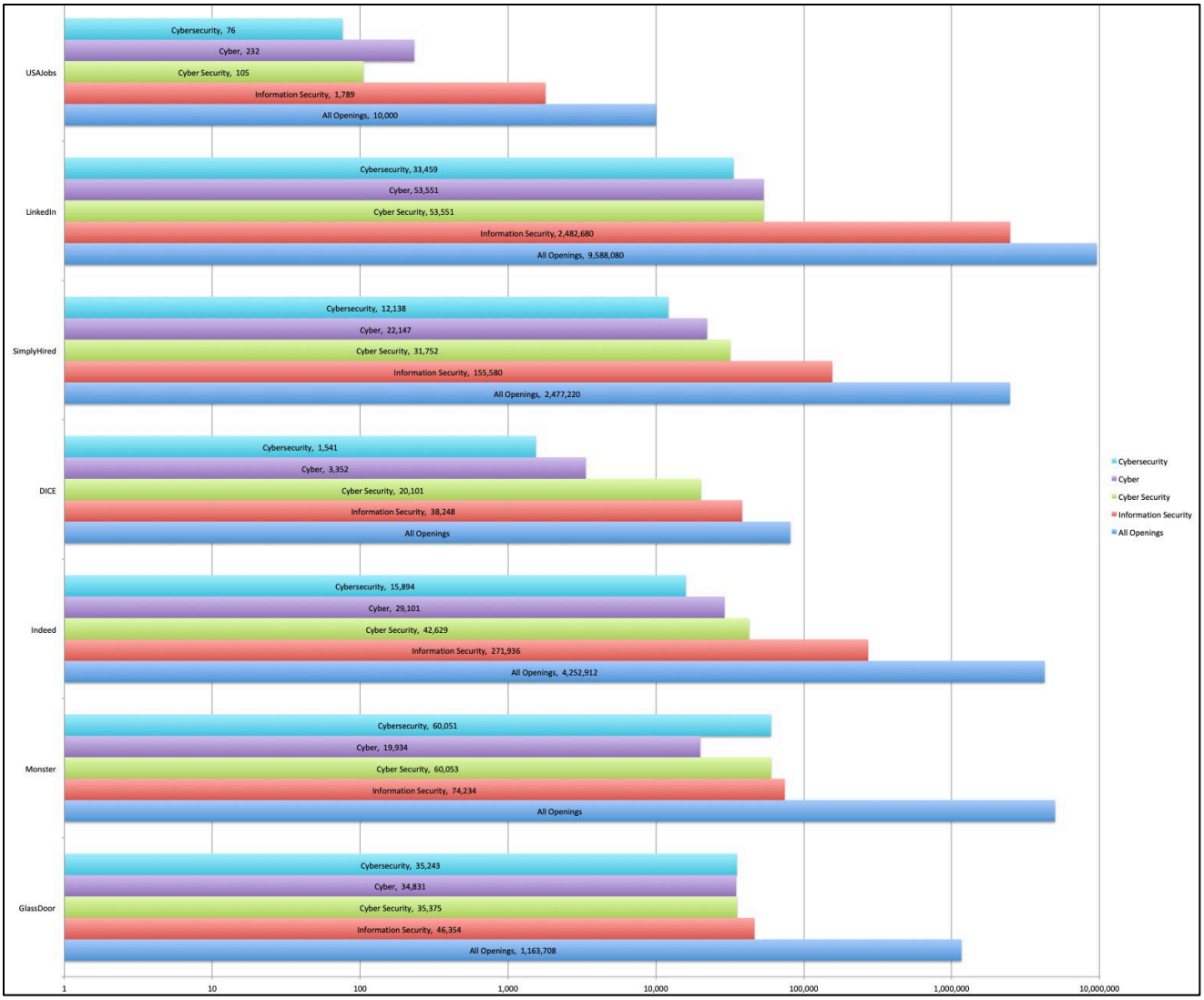

Figure 3: Information Security, Cyber Security, and Cyber search results on job placement boards (November 2018)

IV. Threat Analysis

Since 2008, Verizon has released its annual Data Breach Investigations Report (DBIR), which presents in-depth analysis and valuable insights into tens of thousands of incidents and data breaches across the globe. Handling over 500 security breach and data compromise engagements between 2004 and 2007,[14] their 2018 report now includes over 53,000 security incidents and 2,216 confirmed data breaches from 64 countries.[15] In this document we will review several of these reports to identify cybersecurity job roles that possess the KSAs to fight against these attacks.

Taking note of threats from 5 years ago is a great place to start. We can evaluate how these threats have impacted emerging cybersecurity regulation, business leadership concerns, industry product offerings, threat evolution, and the shaping of the cybersecurity job market. The 2014

DBIR provides a valuable summary of activity from 2009-2013[16]. In that five-year span, several threats are consistently observed. Those include:

- Spyware/Keylogger activity
- Use of stolen credentials
- Brute force attacks
- Backdoor malware
- Backdoor Command and Control (C2)
- Data export malware
- Phishing attacks

Taking these threats into consideration, we will look more closely at the NICE Framework KSAs that are needed to protect against them. Although support roles such as Cyber Instructor (OV-TEA-002) could be leveraged to improve the overall cybersecurity posture of an organization, we will instead focus on identifying more specific roles that address the threats identified within the Verizon reports. In this exercise we highlight the most applicable KSAs for 'preventing' these attacks, along with associated NICE Framework Work Roles. We have grouped similar threats together where the same defensive KSAs would be applicable. The National Initiative for Cybersecurity Careers and Studies (NICCS) website was used for this mapping effort, and could be a valuable resource for similar role definition and mapping for your organization.[17]

Spyware/Keylogger activity

KSA: S00076, Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware)

Work Roles: System Administrator (OM-ADM-001), Security Architect (SP-ARC-002)

KSA: K0536: Knowledge of structure, approach, and strategy of exploitation tools (e.g., sniffers, keyloggers) and techniques (e.g., gaining backdoor access, collecting/exfiltrating data, conducting vulnerability analysis of other systems in the network).

Work Roles: Cyber Operator (CO-OPS-001)

Use of stolen credentials and brute force attacks

KSA: K0284, Knowledge of developing and applying user credential management system.

Work Roles: Systems Security Analyst (OM-ANA-001)

KSA: K0158, Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control).

Work Roles: System Administrator (OM-ADM-001)

KSA: S0121, Skill in system, network, and OS hardening techniques. (e.g., remove unnecessary services, password policies, network segmentation, enable logging, least privilege, etc.).

Work Roles: Cyber Defense Infrastructure Support Specialist (PR-INF-001)

KSA: K0056, Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML)

Work Roles: Systems Security Analyst (OM-ANA-001), Database Administrator (OM-DTA-001), Data Analyst (OM-DTA-002), Cyber Defense Analyst (PR-CDA-001), Vulnerability Assessment Analyst (PR-VAM-001), Enterprise Architect (SP-ARC-001), Security Architect (SP-ARC-002), Security Control Assessor (SP-RSK-002), Systems Requirements Planner (SP-SRP-001), Information Systems Security Developer (SP-SYS-001), Systems Developer (SP-SYS-002)

Backdoor malware, backdoor C2, and data export malware

KSA: S00076, Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware).

Work Roles: System Administrator (OM-ADM-001), Security Architect (SP-ARC-002)

KSA: K0536: Knowledge of structure, approach, and strategy of exploitation tools (e.g., sniffers, keyloggers) and techniques (e.g., gaining backdoor access, collecting/exfiltrating data, conducting vulnerability analysis of other systems in the network).

Work Roles: Cyber Operator (CO-OPS-001)

KSA: K0536: Knowledge of structure, approach, and strategy of exploitation tools (e.g., sniffers, keyloggers) and techniques (e.g., gaining backdoor access, collecting/exfiltrating data, conducting vulnerability analysis of other systems in the network).

Work Roles: Cyber Operator (CO-OPS-001)

Phishing

KSA: K0447, Knowledge of how to collect, view, and identify essential information on targets of interest from metadata (e.g., email, http).

Work Roles: Exploitation Analyst

KSA: S00052, Skill in the use of social engineering techniques. (e.g., phishing, baiting, tailgating, etc.).

Work Roles: Vulnerability Assessment Analyst (PR-VAM-001)

KSA: K0444, Knowledge of how Internet applications work (SMTP email, web-based email, chat clients, VOIP).

Work Roles: All-Source Analyst (AN-ASA-001), Mission Assessment Specialist (AN-ASA-002), Exploitation Analyst (AN-EXP-001), Target Developer (AN-TGT-001), Target Network

Analyst (AN-TGT-002), Threat/Warning Analyst (AN-TWA-001), All-Source-Collection Manager (CO-CLO-001), All Source-Collection Requirements Manager (CO-CLO-002), Cyber Intel Planner (CO-OPL-001), Cyber Ops Planner (CO-OPL-002), Partner Integration Planner (CO-OPL-003)

The 2015 DBIR study observed that 99.9% of exploited vulnerabilities were compromised more than a year after the related Common Vulnerabilities and Exposure (CVE) notice was published. This dramatically reinforces the critical need for properly configured patch management. There are 6 KSAs and Tasks within the NICE Framework that specifically address patching, which are then associated with 9 different Work Roles within the Specialty Areas of Systems Requirements, Systems Architecture, Cyber Operations, Network Services, Systems Analysis, Cyber Defense Analysis, and Software Development.

Building upon this analysis, the 2018 DBIR report adds the use of stolen credentials, privilege abuse, and configuration errors to our list of previously identified threats. Also noted, was ransomware as the top malware variant, which was present in over 45% of incidents in 2017.

Protecting against, and recovering from ransomware has become a crucial need for every organization. In addition to implementing malware protections (S0079), organizations must implement and test backup solutions (S0158) to ensure business continuity if systems and data are completely lost.

KSA: S0158, Skill in operating system administration. (e.g., account maintenance, data backups, maintain system performance, install and configure new hardware/software).

Work Roles: System Administrator (OM-ADM-001)

KSA: S0079, Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).

Work Roles: Network Operations Specialist (OM-NET-001), Cyber Defense Incident Responder (PR-CIR-001), Cyber Defense Infrastructure Support Specialist (PR-INF-001)

Implementing multi-factor authentication is important, and even though it is a DBIR recommendation every year, most organizations fail to take appropriate action. Either the cost is too high, or the tools are too inconvenient. So, although the need for subject matter experts on this topic is high, the demand for those skills appears to be low, simply because organizations are choosing to accept the risk. Conversely, attackers are taking advantage of this. Relevant authentication KSAs have been presented earlier in this document, but we will add one additional Task that addresses this specific issue:

Task: T0446, Design, develop, integrate, and update system security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation.

Work Roles: Information Systems Security Developer (SP-SYS-001)

Another key observation made in the 2018 DBIR is that many two-factor authentication systems leverage companion applications installed on mobile phones. This further emphasizes the need to

have subject matter experts to securely architect mobile device management solutions, along with others that have the knowledge and skills to properly investigate mobile-related incidents. These needs tie back to (ISC)² Global Cybersecurity studies that highlight mobile device concerns.

Relevant mobile-related KSAs include:

KSA: K0269, Knowledge of mobile communications architecture.

Work Roles: Research & Development Specialist (SP-TRD-001)

KSA: S0075, Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems).

Work Roles: Law Enforcement/Counterintelligence Forensics Analyst (IN-FOR-001), Cyber Defense Forensics Analyst (IN-FOR-002)

Given our KSA analysis for threat prevention, our Top 5 NICE Framework Work Roles in demand are:

- Cyber Defense Analyst (PR-CDA-001)
- Cyber Operator (CO-OPS-001)
- Security Architect (SP-ARC-002)
- System Administrator (OM-ADM-001)
- System Security Analyst (OM-ANA-001)

The *Systems Administrator* and *System Security Analyst* demand is further validated by Cyberseek.org data from September 2017 – August 2018, which identify those Work Roles within the top 10 requested job titles by employers. However, when reviewing our NICE Framework Work Role text queries of popular employment sites, only *System Administrator* consistently made the top 10 results.[18]

It is a common notion that cyber incidents are inevitable. It is no longer if a compromise will occur, but when. Several reports, including Cisco's 2014, "Mitigating the Cybersecurity Skills Shortage," highlight the need to develop incident handling skills throughout your organization.[19] We have just reviewed a number of important KSAs focused on threat prevention, but it is worth noting that there are over 40 KSAs and Tasks related to incident detection and handling within the NICE Framework. Clear mappings exist to Work Roles such as the Cyber Defense Incident Responder (PR-CIR-001), but there is the potential for nearly every role within the framework to be impacted, including Executive Cyber Leadership (OV-EXL-001). This need is further emphasized in (ISC)² 2017 Global Workforce Study, in which 52% of the survey respondents felt incident investigation and response was a top needed area of expertise.[20]

V. Managed Security Services

Technology is constantly progressing. Unfortunately cybersecurity threats are also continuously evolving to target weaknesses in these new capabilities. It is difficult for today's workforce to keep up with the challenging pace. Managed Security Services (MSS) can be a valuable resource if organizations are overtasked, understaffed, or if they have difficulty finding the talent or budget to grow in-house capabilities.

Intel Security along with the Center for Strategic and International Studies (CSIS) released their "Hacking the Skills Shortage" global report in 2016, which also highlighted the talent shortage crisis. 82% of respondents from 8 countries felt there were shortages within their organization, as well as their respective countries. Highlighted within this report was that 67% of U.S. respondents outsource their threat detection. This closely correlates to the 74% of U.S respondents that also identified intrusion detection as a scarce skill.[21] These points, along with those made in the (ISC)[2] studies regarding the increased usage of external service providers, necessitate taking a closer look at MSS capabilities and workforce needs.

An MSS Provider (MSSP) often acts as an extension of an organization's security operation, and can be used to address cost, complexity, and availability challenges. The 2018 Magic Quadrant report stated, "The MSS market constitutes approximately 60% of the overall security outsourcing market that will generate $18.7 billion revenue in 2017, growing at a CAGR of 11% through 2021."[22] Typical MSSP offerings include:

> "Security event monitoring only, or security event monitoring along with device/agent monitoring and management, primarily in the following categories: Firewalls, Network-based threat detection technologies, such as network intrusion detection/prevention systems (IDPS), Multifunction firewalls, or unified threat management (UTM) technology, Security gateways for messaging or web traffic, Web application firewalls, Endpoint protection platforms (EPPs), host intrusion detection/prevention systems (HIDS/HIPS) and endpoint detection and response (EDR); Security analysis and reporting of events collected from IT infrastructure and application logs; Reporting for service management, regulatory compliance requirements and threat detection purposes; Management and monitoring, or monitoring only of advanced threat defense technologies, or the provision of those capabilities as a service; Management and monitoring of customer-deployed security information and event management (SIEM) technologies; Incident response services (both remote and on-site)."

NICE Framework Work Roles that can easily be mapped to listed MSSP capabilities include:

- Cyber Defense Incident Responder (PR-CIR-001)
- Cyber Defense Forensics Analyst (IN-FOR-002)
- Network Operations Specialist (OM-NET-001)
- Security Control Assessor (SP-RSK-002)

- Information Systems Security Manager (OM-NET-001)
- Vulnerability Assessment Analyst (PR-VAM-001)
- Information Systems Security Developer (SP-SYS-001)
- Research & Development Specialist (SP-TRD-001)

Although we can infer these connections, we continue to see that most organizations have not adopted a consistent standard for defining cybersecurity positions. To better understand this lexicon challenge, let us take a brief look at November 2018 cybersecurity job postings for the leaders and visionaries from the 2018 Gartner MSS Magic Quadrant report for MSSPs. These were SecureWorks, IBM, Symantec, Verizon, and Trustwave.

SecureWorks had just over 7,000 jobs available. Text-based queries on "cyber security" and "cybersecurity" displayed 248 and 318 results respectfully, while "information security" resulted in a whopping 1,665 postings. This quickly highlights that the term "cyber" has not yet been fully embraced by industry. We also saw this in our analysis of popular job sites where "information security" more than tripled the search results of the other aforementioned terms.[23] Additional queries and analysis on the SecureWorks site showed 24% of their current openings (1,706) were for operations and/or technical consultants, cloud security analysts, and solutions engineers.

IBM had over 6,800 jobs posted, with almost 24% within their "Technical Specialist" category (1,628). Other categories like "Architect" included numerous software development positions for mobile and automation, along with Systems Administration and Cyber Threat Responder. Their "Software Development and Support" category made up just over 11% of their current openings.

Symantec's site listed 311 jobs. Similar to the previous MSSPs there were no high-level categories that directly mapped to cybersecurity related functions. The "Information Technology Function" included 13% of their open positions and encompassed descriptions such as Researcher, Analyst, Admin, Developer, and Manager. Their "Development" function more than doubled the next closest category at 31% of their openings (97).

Verizon offered 2,196 openings at the time of our November queries. Almost 24% of those were listed as Technology (388) or Systems/Data Security (130). Only 25 "Security Engineer" positions were returned among the thousands available, and with a wide variety of categories including network security, physical access, application, cloud, Network Security Operations Center, and systems/data security.

Trustwave's careers page listed 47 current openings. 38% were on their "Security Services" team (18) with job titles such as "Security Consultant" and "Information Security Advisor."

The average number of cybersecurity-like positions found during our November 2018 queries of the 5 Leaders of the Gartner MSSP Magic Quadrant indicate around 25% of their current job openings were cybersecurity related. We also observed significant openings for software development professionals, and noticeable needs in areas of cloud and mobile solution security.

Perhaps the most telling observation of all was that there was absolutely no consistency across these providers for categorizing and defining cybersecurity work roles.

VI. Technology Trends

After looking at existing job postings, and identifying high-demand roles based on threats, we found it prudent to investigate key technology trends, and how those reinforce specific cybersecurity needs.

IoT

According to Gartner, the Internet of Things (IoT) is, "The network of physical objects that contain embedded technology to communicate and sense or interact with the internal states or external environment."[24] Basically, our world has become extremely connected. From wearable devices such as an Apple Watch[25] or FitBit[26] that monitor heart rates and movement, to smart meters and devices in your home that report environmental and performance data, to production networks of devices that control traffic lights, and utilities. Almost everything is connected to a telecommunications network, with some estimates predicting 30 billion connected devices by 2020.[27] This "convenience" also introduces vulnerabilities as misconfigured devices or improper error handling within software could lead to the compromise of sensitive information. Even worse, failure to implement fundamental cybersecurity controls, like strong password authentication and encrypted protocols, could lead to malicious attacks.[28]

Symantec's 2018 Internet Security Threat Report found a 600% increase in overall IoT attacks in 2017.[29] To protect our IoT there are several important considerations. First, it is necessary to develop inherently secure software. No one (and no software) is perfect, so there needs to be an easy, efficient, and secure way to update those applications and devices. Cybersecurity experts will also be challenged to understand how IoT devices communicate, what protocols are used, what services are running, and what security and/or privacy settings can be configured.

The following KSAs and Work Roles are expected to play a greater role in the cybersecurity landscape as IoT devices continue to evolve.

KSA: A001, Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.

Work Roles: Vulnerability Assessment Analyst (PR-VAM-001)

KSA: A0046, Ability to monitor and assess the potential impact of emerging technologies on laws, regulations, and/or policies.

Work Roles: Cyber Legal Advisor (OV-LGA-001)

KSA: A0047, Ability to develop secure software according to secure software deployment methodologies, tools, and practices.

Work Roles: Software Developer (SP-DEV-001)

KSA: K0174, Knowledge of networking protocols.

Work Roles: Research & Development Specialist (SP-TRD-001)

KSA: K0178, Knowledge of secure software deployment methodologies, tools, and practices.

Work Roles: Secure Software Assessor (SP-DEV-002)

KSA: S0182, Skill in analyzing target communications internals and externals collected from wireless LANs.

Work Roles: Cyber Operator (CO-OPS-001)

KSA: S0184, Skill in analyzing traffic to identify network devices.

Work Roles: Security Control Assessor (SP-RSK-002), Exploitation Analyst (AN-EXP-001)

There are numerous other applicable KSAs that could be referenced to support IoT. However, the key takeaway for IoT is that these emerging technologies require Software Developers (SP-DEV-001), Researchers (SP-TRD-001), Legal Advisors (OV-LGA-001), Security Control Assessors (SP-RSK-002), Cyber Operators (CO-OPS-001), along with specialists and technicians at many levels to continuously learn and adapt their tools, techniques, and procedures to best support and protect devices, users, and their organizations.

The Cloud

There are many definitions for, "The Cloud." This is partly because there are many methods for deploying, managing, and utilizing computing services. For example, the Software as a Service (SaaS) cloud model includes applications like Microsoft Office 365 and Google Docs that are hosted entirely on vendor infrastructure using their software. Your organization may instead choose to host your own applications using Google, Amazon, Microsoft, or another service provider's equipment using Platform as a Service (PaaS) or Infrastructure as a Service (IaaS) models. These Cloud services help organizations meet scalability, availability, and reliability needs without having to invest in capital equipment expenses. While Cloud solutions can offload some of the technology management overhead, they do not allow a company to transfer legal or financial risk and liability. Cloud solutions still require the same level of protection as traditional infrastructures. Applications and operating systems still need to be properly patched, regardless of who is performing the update. Furthermore, controls for authentication, access, anti-virus, network segmentation, and other best practices must to be implemented. Additionally, security audits and network assessments need to be completed to ensure the best possible security posture, and these often take coordination with Cloud service providers.

There are 9 NICE Framework KSAs and Tasks that specifically reference the Cloud. Here we highlight just a few critical ones along with their related Work Roles.

KSA: A001, Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.

Work Roles: Vulnerability Assessment Analyst (PR-VAM-001)

KSA: A0121, Ability to design incident response for cloud service models.

Work Roles: Cyber Defense Incident Responder (PR-CIR-001)

KSA: S0073, Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.).

Work Roles: Security Control Assessor (SP-RSK-002), System Administrator (OM-ADM-001), Cyber Defense Forensics Analyst (IN-FOR-002)

Task: T0251, Develop security compliance processes and/or audits for external services (e.g., cloud service providers, data centers).

Work Roles: Security Control Assessor (SP-RSK-002)

Automation, Artificial Intelligence (AI), and Machine Learning (ML)

The McKinsey Global Institute released a report in December of 2017, which estimated that Automation could destroy as many as 73 million jobs in the U.S. by 2030.[30] Companion scenarios and models within the study demonstrate the potential for new, more skilled jobs to be created as automated technologies are implemented and economies grow. Furthermore, studies indicate that the AI market could exceed $5 billion by 2020, and AI software that supports ML will grow to almost $60 billion by 2025.[31] Although cybersecurity related automation is not explicitly called out within these sources, we can deduce the need for Software Developers (SP-DEV-001), Secure Software Assessors (SP-DEV-002), and Research & Development Specialists (SP-TRD-001), along with work roles that support the underlying operations and infrastructure for automation, AI, and ML.

Cisco's 2018 Annual Cybersecurity Report analyzes survey results from over 3600 cybersecurity practitioners. Highlighted within the report is that 39% of security professionals said they are reliant on automation, 34% on machine learning, and 32% artificial intelligence to defend their networks.[32] The primary purpose of these advanced capabilities is to enhance cyber defenses and learn how to automatically detect unusual patterns. With over a million new pieces of malware created each day,[33] automating analysis and configuration updates becomes paramount to protecting the organization.

Security can be further enhanced as part of Development Operations (DevOps), which combine software development methodologies with continuous IT integration. Incorporating automated testing techniques, such as fuzzing and software penetration testing can identify potential issues early in the software development cycle, before they are exposed to malicious threat actors.[34]

Increased autonomy can improve cybersecurity by providing a mechanism for handling large data volumes, at high speeds, using consistent methodologies. However, algorithms and AI/ML applications are still dependent on the availability of large sets of data. Networks and systems will need to be instrumented to support this collection. Thus, requiring support from traditional IT roles such as System Administrators (OM-ADM-001), Network Operations Specialists (OM-NET-001), and Cyber Operators (CO-OPS-001). Furthermore, as dependence on these systems is established, it will be necessary to ensure they are hardened against attacks, assessed for vulnerabilities, and monitored for unacceptable actions.

In addition to the previously mentioned NICE Framework roles, including the following KSAs within your organization will enhance AI, ML, and Automation security:

KSA: A001, Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.

Work Roles: Vulnerability Assessment Analyst (PR-VAM-001)

KSA: A0030, Ability to collect, verify, and validate test data.

Work Roles: System Testing and Evaluation Specialist (SP-TST-001)

KSA: K0238, Knowledge of machine learning theory and principles.

Work Roles: Data Analyst (OM-DTA-002)

Regulations, Mandates, and Initiatives

There are numerous elements influencing cybersecurity requirements. These in turn necessitate the implementation of tools and procedures to achieve compliance. And of course, these require people available to perform the required tasks. Whether these professionals are on-staff or outsourced, the capabilities must be available to an organization and the appropriate cybersecurity actions must be taken. In this section we will take a look at several regulations and laws impacted by recent cyber threats and strategic initiatives. In doing so, we will highlight additional NICE Framework KSAs and Work Roles that support these efforts.

The Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996 and establishes standards for electronic data exchange, along with privacy and security standards for health information.[35] The primary objective of the Security Rule within HIPAA is to protect privacy of health information while adopting new technologies intended to improve the quality and efficiency of patient care. Adding to these security challenges is that hospitals have become one of the largest targets for malicious cyber attacks. According to a 2018 report from global cybersecurity insurance company Beazley, 45% of all ransomware attacks targeted the healthcare industry.[36]

To help combat these and other threats, the Department of Health & Human Services has developed several resources including a Cyber Security Checklist, Cyber Security Infographic, and Ransomware Guidance.[37] Within these resources are recommendations to limit access to electronic protected health information (ePHI) to only persons and applications with a need-to-know. We also see the needs highlighted for performing risk assessments, providing cybersecurity training to users, and installing applications to guard against malicious software. Among other things, the ransomware guidance calls out HIPAA requirements to have procedures for responding and reporting security incidents in place.

Identifying the list of KSAs and Work Roles required for securely operating a healthcare organization would be a near complete listing of the NICE Framework. However, we will refer back to our previously mentioned roles that would be instrumental in protecting and recovering from a malware/ransomware incident. These include System Administrator (OM-ADM-001),

Network Operations Specialist (OM-NET-001), Cyber Defense Incident Responder (PR-CIR-001), and Cyber Defense Infrastructure Support Specialist (PR-INF-001).

The Sarbanes-Oxley Act was signed into law in 2002, and is primarily designed to oversee financial reporting for publicly held companies. However, the scope of these requirements is continuing to evolve. In 2016 the Cybersecurity Systems and Risks Reporting Act was introduced, and then followed-up by related disclosure guidance from the U.S. Securities and Exchange Commission (SEC) in 2018.[38] According to the global consulting firm Protiviti's 2018 Sarbanes Oxley Compliance Survey of more than 1000 publicly held organizations, the percentage of organizations having to provide cybersecurity disclosures was 46%, which demonstrated a 13% increase for the second consecutive year.[39] The ability to author a privacy disclosure statement based on current laws (A0125) is associated with the Privacy Officer/Privacy Compliance Manager (OV-LGA-002) role within the NICE Framework.

The European Union (EU) General Data Protection Regulation (GDPR) went into effect in May 2018.[40] In general, GDPR is intended to protect the personal data of European citizens. This applies to all companies processing personal data of subjects residing in the EU regardless of where that company's location is. Key elements include breach notification requirements, and a person's ability to access all of their digital data, as well as their right to be forgotten. GDPR introduces the need to appoint a Data Protection Officer (DPO), which helps monitor internal compliance and must be an expert in data protection. This role most closely maps to the Privacy Officer/Privacy Compliance Manager (OV-LGA-002) within the NICE Framework.

Another example of legislation defining cybersecurity needs is the National Cybersecurity and Critical Infrastructure Protection Act of 2014. This bill amends the Homeland Security Act of 2002 to provide DHS additional authorities regarding the protection of federal civilian information systems and the ability to support requests to protect critical infrastructure or to assist response and recovery from cyber threats.[41] This responsibility falls on the shoulders of many people and many different positions. Here is an example of one critical infrastructure Ability, which is important enough to be linked to 11 different Work Roles.

KSA: A0170, Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations.

Work Roles: Information Systems Security Manager (OM-NET-001), Enterprise Architect (SP-ARC-001), Security Architect (SP-ARC-002), Software Developer (SP-DEV-001), Secure Software Assessor (SP-DEV-002), Authorizing Official/Designating Representative (SP-RSK-001), Security Control Assessor (SP-RSK-002), Systems Requirements Planner (SP-SRP-001), Information Systems Security Developer (SP-SYS-001), Systems Designer (SP-SYS-002), Research & Development Specialist (SP-TRD-001)

With the examples noted above, we can see how regulations, mandates, and national strategies impact the cybersecurity workforce. By defining minimum network, system, and data security requirements for organizations, in turn, establishes a set of essential knowledge, skills, and abilities for the cybersecurity professionals required to perform related tasks. Similarly, other

roles are inherently needed to validate controls and protections are properly implemented. Those skills in governance, risk management, and compliance were identified by 38% of the 2017 (ISC)² Global Information Security Workforce Study respondents as skills needed for advancing their career.[42]

VII. The Cybersecurity Workforce of the Future

In our analysis we have mentioned numerous KSAs and Work Roles, which are essential today, and for improving our nation's cybersecurity posture in the future. Here is a recap of the top identified roles:

Top 10 Work Roles based on Threats, Regulation, and Emerging Technology Needs

- Information Systems Security Manager (OM-NET-001)
- System Administrator (OM-ADM-001)
- Cyber Defense Incident Responder (PR-CIR-001)
- Cyber Defense Analyst (PR-CDA-001)
- Vulnerability Assessment Analyst (PR-VAM-001)
- Security Architect (SP-ARC-002)
- Systems Developer (SP-SYS-002)
- Software Developer (SP-DEV-001)
- Information Systems Security Developer (SP-SYS-001)
- Security Control Assessor (SP-RSK-002)
- Research & Development Specialist (SP-TRD-001)

Top 10 Work Roles based on queries of popular employment web sites

- Knowledge Manager (OM-KMG-001)
- All Source-Collection Requirements Manager (CO-CLO-002)
- IT Project Manager (OV-PMA-002)
- Information Systems Security Developer (SP-SYS-001)
- Information Systems Security Manager (OV-MGT-001)
- Systems Developer (SP-SYS-002)
- All Source-Collection Manager (CO-CLO-001)
- Product Support Manager (OF-PMA-003)

- Research & Development Specialist (SP-TRD-001)
- Software Developer (SP-DEV-001)

Top Job Titles requested by employers as per Cyberseek.org

- Cyber Security Engineer
- Cyber Security Analyst
- Network Engineer / Architect
- Cyber Security Manager / Administrator
- Systems Engineer
- Software Developer / Engineer
- Systems Administrator
- Vulnerability Analyst / Penetration Tester
- Cyber Security Consultant

Note: Multiple NICE Framework Work Roles were consolidated within the Cyberseek.org 'Job Title' listings.

Given these three lists, we will now identify the Top 5 in-demand cybersecurity Work Roles. These are:

Information Systems Security Developer (SP-SYS-001)

This Work Role was #4 on our aggregated job site search results, and with more than 130 KSAs and Tasks, it is one of the most comprehensive. It rated highly on our MSSP review and is responsible for designing, developing, testing and evaluating information systems security through a systems development life cycle.

Information Systems Security Manager (OV-MGT-001)

This role is responsible for the cybersecurity of a program, organization, system, or enclave and came in at #5 on our aggregated job site search results. Worth noting was that three of the top five results on USAJobs.gov were "manager" positions. One potential reason for this is the government's tendency to outsource technical roles, while providing the managerial oversight to those activities.

Systems Developer (SP-SYS-002)

This Work Role has numerous KSAs that support threat prevention, identifying vulnerabilities, integrating secure software/hardware solutions, and building product prototypes. It was at #6 on the aggregated job search, while also being one of the Cyberseek's top requested job positions.

Research & Development Specialist (SP-TRD-001)

Although this Work Role came in 8th on our aggregated job site results, it is critical in the support of emerging technologies, identifying threats and vulnerabilities, and integrating cybersecurity within systems, networks, and other solutions.

Software Developer (SP-DEV-001)

One could argue that "cyber" does not exist without software. This Work Role develops, creates, and maintains applications. Aggregated search results of job sites only had this role at #9, but there are so many other descriptions for software developer like engineer or architect, which could easily be added to those results. The cybersecurity market is expected to reach $172 Billion by 2022[43], and many of those services depend on software solutions. Furthermore, the Bureau of Labor Statistics estimates over 1.2M Software Developer jobs within the U.S. with an expected growth rate of 24% through 2026.[44]

Although we have identified our Top 5, we have several other roles that absolutely must be mentioned. As discussed in the Automation, AI, and ML section, System Administrators (OM-ADM-001), Network Operations Specialists (OM-NET-001), and Cyber Operators (CO-OPS-001) are required to provide the underlying telecommunication and computing services that are the core of today's businesses. Likewise for all organizations, systems need to be implemented to meet functional needs. However, they must also be deployed in a manner that is efficient and secure. These Work Roles provide fundamental building blocks for the more advanced cybersecurity positions, and these professionals are often responsible for performing cyber-related tasks.

High volumes of cyber incidents, along with our dependence on technology for critical infrastructure, financial systems, health networks, and medical devices have prompted demand for increased security. Regulators, lawmakers, and citizens require assurance that their safety and information are properly protected. Current and emerging requirements for risk, compliance, and security assessments highlight the growing need for professionals in the roles of Vulnerability Assessment Analyst (PR-VAM-001) and Security Control Assessor (SP-RSK-002).

VIII. Call to Action

Our research highlights the inconsistencies between position descriptions, job categories, and mappings to any one framework. Cyberseek is a great resource for informing the cybersecurity workforce, but it does not provide access to related job postings. Conversely, employment services and corporate web resources list available positions, but they do not adequately map their openings to the NICE Framework or any other framework. Both employers and job candidates would benefit immensely by the adoption of a common lexicon. Job postings need to be categorized and tagged in a way that maps to a single standard.

The NICE Framework provides such a foundation. It has adoption within the U.S. Federal government as well as the Department of Defense and is being leveraged internationally. If fully

embraced, it can provide a consistent guide and road map for perspective employers, educators, and cybersecurity professionals.

Specific recommendations include:

- Ensure USAJobs.gov categorizes and/or tags all available positions in a manner consistent with the NICE Framework. Government adoption and integration must be 100%.
- U.S. Department of Labor – Bureau of Labor Statistics has to recognize NICE Framework roles within their Occupational Outlook Handbook.
- Job placement services and websites need to adopt a common cybersecurity workforce framework for work role identification. That framework should be the NICE Framework.
- DHS should continue to refine and promote their PushButtonPD™ tool,[45] which could lead to better adoption of the NICE Framework, while also producing consistent cybersecurity position descriptions throughout the community.
- Request (ISC)² and Frost & Sullivan to expand NICE related survey questions to the broader, non-U.S. Government organizations and publish those results in future studies.
- High schools and higher education institutions need to adopt consistent curriculums that include the KSAs tied to the following NICE Framework Work Roles:
    - Information Systems Security Manager (OV-MGT-001)
    - Information Systems Security Developer (SP-SYS-001)
    - Systems Developer (SP-SYS-002)
    - Software Developer (SP-DEV-001)
    - Vulnerability Assessment Analyst (PR-VAM-001)
    - Security Control Assessor (SP-RSK-002)
    - Cyber Operator (CO-OPS-001)
    - System Administrator (OM-ADM-001)
    - Network Operations Specialist (OM-NET-001)
    - Research & Development Specialist (SP-TRD-001)

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM19-0008

[1] https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx (Retrieved December 2018)
[2] https://www.isc2.org/about
[3] https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx (Retrieved December 2018)
[4] https://www.isc2.org/-/media/Files/Research/GISWS-Report-US-Govt-2017.ashx (Retrieved December 2018)
[5] https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework (Retrieved December 2018)
[6] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf (Retrieved December 2018)
[7] Office of Personnel Management, Memorandum for Heads of Executive Departments and Agencies: Guidance for Assigning New Cybersecurity Codes to Positions with Information Technology, Cybersecurity, and Cyber-Related Functions (Washington, D.C.: January 4, 2017), https://www.gao.gov/assets/700/692498.pdf (Retrieved December 2018)
[8] https://dodcio.defense.gov/Cyber-Workforce/dcwf.aspx (Retrieved December 2018)
[9] https://www.nist.gov/itl/applied-cybersecurity/nice/nice-spring-2018-enewsletter (Retrieved December 2018)
[10] https://www.gooduniversitiesguide.com.au/education-blogs/guest/building-the-cyber-security-workforce-australia-needs (Retrieved December 2018)
[11] https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm (Retrieved December 2018)
[12] https://www.cyberseek.org (Retrieved December 2018)
[13] November/December 2018 – Glassdoor.com, Indeed.com, Monster.com, LinkedIn.com, Dice.com, SimplyHired.com, USAJobs.gov (see spreadsheet)
[14] http://www.verizonenterprise.com/resources/security/databreachreport.pdf (Retrieved December 2018)
[15] https://enterprise.verizon.com/resources/reports/dbir/ (Retrieved December 2018)
[16] http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf (Retrieved December 2018)
[17] https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework/search (Retrieved December 2018)
[18] November/December 2018 – Glassdoor.com, Indeed.com, Monster.com, LinkedIn.com, Dice.com, SimplyHired.com, USAJobs.gov (see spreadsheet)
[19] https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf (Retrieved December 2018)
[20] https://www.isc2.org/Research/Workforce-Study (Retrieved December 2018)
[21] http://mcafee.com/skillsshortage (Retrieved December 2018)
[22] Gartner "2018 Magic Quadrant for Managed Security Services, Worldwide" by Toby Bussa, Kelly M. Kavanagh, Sid Deshpande, Pete Shoard, Published: 27 February 2018.
[23] November/December 2018 – Glassdoor.com, Indeed.com, Monster.com, LinkedIn.com, Dice.com, SimplyHired.com, USAJobs.gov (see spreadsheet)
[24] Gartner IT Glossary, "Internet of Things," https://www.gartner.com/it-glossary/internet-of-things/ (Retrieved December 2018)
[25] https://www.apple.com/watch/ (Retrieved December 2018)
[26] https://www.fitbit.com (Retrieved December 2018)
[27] https://www.mckinsey.com/featured-insights/internet-of-things/our-insights/six-ways-ceos-can-promote-cybersecurity-in-the-iot-age
[28] https://www.csoonline.com/article/3124344/internet-of-things/armies-of-hacked-iot-devices-launch-unprecedented-ddos-attacks.html
[29] https://interactive.symantec.com/ISTR
[30] https://www.mckinsey.com/~/media/mckinsey/featured%20insights/future%20of%20organizations/what%

20the%20future%20of%20work%20will%20mean%20for%20jobs%20skills%20and%20wages/mgi-jobs-lost-jobs-gained-report-december-6-2017.ashx (Retrieved December 2018)

[31] https://blog.capterra.com/machine-learning-and-artificial-intelligence-statistics/ (Retrieved December 2018)

[32] https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf (Retrieved December 2018)

[33] https://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/index.html (Retrieved December 2018)

[34] https://insights.sei.cmu.edu/devops/2016/11/an-introduction-to-secure-devops-including-security-in-the-software-lifecycle.html (Retrieved December 2018)

[35] https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (Retrieved December 2018)

[36] https://www.beazley.com/documents/Whitepapers/201802-beazley-breach-briefing.pdf (Retrieved December 2018)

[37] https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity (Retrieved December 2018)

[38] https://www.sec.gov/rules/interp/2018/33-10459.pdf (Retrieved December 2018)

[39] https://www.protiviti.com/sites/default/files/united_states/insights/sarbanes-oxley_survey_2018_protiviti.pdf (Retrieved December 2018)

[40] https://eugdpr.org/the-regulation/gdpr-faqs/ (Retrieved December 2018)

[41] https://www.congress.gov/bill/113th-congress/house-bill/3696 (Retrieved December 2018)

[42] https://www.isc2.org/-/media/Files/Research/GISWS-Report-US-Govt-2017.ashx (Retrieved December 2018)

[43] https://www.marketwatch.com/press-release/cyber-security-market-to-touch-us-170-billion-by-2022-2018-08-26

[44] https://www.bls.gov/ooh/computer-and-information-technology/software-developers.htm (Retrieved December 2018)

[45] https://niccs.us-cert.gov/workforce-development/cybersecurity-resources/dhs-pushbuttonpd-tool (Retrieved December 2018)