CERT
Software Engineering Institute
Carnegie Mellon University

STRIVING FOR EFFECTIVE CYBER WORKFORCE DEVELOPMENT

Marie Baker

May 2016

Executive Summary

The United States is in a critical situation in terms of cyber preparedness. Cyber attacks and their sophistication are growing exponentially, while the cyber workforce is striving to strengthen and sustain the talent needed to protect, detect, defend, and respond to these attacks. Effective cyber workforce development – increasing the number of qualified professionals in the field and having the right tools to advance their prowess in information security operations – is challenging.

The first challenge, awareness, is two-fold. It is both lack of awareness of career opportunities within the cyber field, and inadequacy of awareness of vigilant security practices within the existing cyber workforce, which is essential to safeguarding the confidentiality, integrity, and availability of information technology environments.

The second challenge is the uncertainty of operator preparedness within the cyber workforce. Neither criteria to assess the qualifications of an individual, nor the skillsets needed to proficiently perform one's duties, is firmly established. An educated, talented, security-minded cyber workforce is essential as the nation has become deeply dependent on cyberspace, and the realization of attacks is a risk with detrimental consequences to critical services in every sector.

In response to this crisis and the potential threat to U.S. security, several cyber workforce development initiatives have been established to grow, train, and retain a pool of highly skilled cyber professionals. A survey of some of these initiatives, specifically awareness and training programs, are described in this white paper, along with a sampling of projects that support these efforts. While these initiatives are mechanisms designed to address shortcomings in cyber workforce development – awareness of, and proficiency in, the cyber career field – the campaigns have yet to solve the issues on an impactful scale.

The number of qualified individuals needed to join the cyber workforce continues to grow, while there are concerns that not enough viable candidates are pursuing this career path. The current weaknesses in awareness of cyber career opportunities as well as cybersecurity awareness in the existing workforce, are having negative effects on the industry. This paper reviews the issue of cyber awareness and identify efforts to combat this deficiency.

Finally, training standards and competency assessment for those already in cyber positions are still being defined and developed. There is an absence of measurable criteria to validate that an operator is proficient in the skills needed to successfully perform their job duties. A survey of initiatives to

consistently describe cyber workforce roles and responsibilities, and apply metrics to targeted training plans, are reviewed.

Effective cyber workforce development is attainable. The two hurdles, lack of awareness and training standards, can be overcome. If the importance of cybersecurity continues to be lauded as a national priority, and the strategies underway with available resources are utilized by intended audiences, effective cyber workforce development is a goal that can be realized.

1 Introduction

The cyber domain is the fabric of the 21st century's global economy and Americans are almost universally dependent on it for most aspects of daily life. This trend steadily increases as software and ubiquitous, perpetually-connected gadgets and devices control most aspects of daily life. Critical services, resources, and operations are contingent upon the availability and reliability of networked connectivity. This reliance on networked systems and applications makes us vulnerable to devastation in the wake of a cyber attack.

The regular publications of cyber attacks in recent years have served as an undeniable recognition of the complexity and power of cyber weapons, and demonstrates the maturity of malicious code and its ability to impact operations on a grand scale. The threat is far reaching and all encompassing. From data and identity theft, to utilities and ecommerce, to nuclear facilities, vulnerabilities exist and have consequences on individual, local, and global levels.

While the acknowledgement of the urgency of the situation is no longer a concern reserved just for the national security community, the number of skilled cybersecurity professionals, and the confidence in the preparedness to handle a major cyber attack has remained low. In a 2010 interview, James Gosler, a veteran cybersecurity specialist who has worked at several government agencies, warned that there is a lack of sufficiently bright people moving into fields that support national cybersecurity objectives, and the number of skilled cybersecurity professionals would need to grow to between 20,000 and 30,000. Five years later, in 2015, Cisco reported there to be one million cybersecurity job openings globally, and the CEO at the security software vendor, Symantec, says that global demand is expected to rise to 6 million by 2019.

Other countries' aggressive cyber tactics and prioritization of becoming leaders in cyber expertise exacerbate the situation. According to Verizon's *Data Breach Investigation Report*, published yearly, researchers examine security incidents and routinely find that a good percentage of the reported incidents were carried out by state-affiliated hackers on espionage missions, most of which can be tracked back to China.

Because of the potential crippling effect of an exploited vulnerability on critical infrastructure industries, and the need to compete globally in areas of cyber expertise, great emphasis has been placed on having a skilled cyber workforce that is prepared to perform defensive and offensive operations in cyberspace. Numerous initiatives for cybersecurity awareness and training have been established in an effort to cultivate a talented cyber workforce.

This document highlights two areas of cyber workforce development: awareness and training. People need to be made aware of the career field and the hundreds of thousands vacant cyber security positions. Awareness also in terms of sound computing practices for the existing workforce to strengthen the human element of cyber operations. Some of the awareness initiatives, including those targeted at minorities and the younger population, are reviewed. The second area of cyber workforce development highlighted is training. Several cyber workforce training and development plans, and their approaches to supporting the goal of creating a robust cybersecurity workforce are surveyed. This paper concludes with strategies moving forward to enhance current awareness and training programs to aid in growing the cyber workforce, and ensuring operational preparedness.

1.1 Purpose and Scope

This paper summarizes the current posture of the cyber workforce and several of the initiatives designed to strengthen, grow, and retain cybersecurity professionals. The purpose of this paper is to highlight cyber workforce development efforts in awareness and training that are designed to address the shortage of skilled cybersecurity professionals, and prepare the workforce to operate offensive and defensively in cyberspace.

1.2 Audience

The audience of this paper includes individuals with a stake in cybersecurity workforce development, and professionals with the opportunity of advancing themselves or others in the cyber field. Whether used by a manager of an organization with a significant cyber footprint, a leader in government or military sectors, or members of the cyber workforce investing in their future in cybersecurity operations, the information contained in this paper should serve as a resource for current activities, trends, and a view of strategies moving forward.

1.3 Document Structure

The introduction presents specific examples and explanations of why cybersecurity is so concerning on a national level and why it’s imperative to develop and retain a skilled cybersecurity workforce. This document then reviews several awareness campaigns aimed at reaching various communities and instilling an understanding of, and interest in, career opportunities in cyber operations. The only way to fill open positions in the cyber field, and get the pipeline of individuals pursuing careers in the field flowing, is to ensure communities are aware of the opportunities and the importance of this work. Cybersecurity awareness for the existing workforce and the impact of the human element on secure operations, is included. Next, several training and development initiatives are described. These initiatives aim to define training standards for the cyber workforce in an effort to foster consistently skilled operators. The paper concludes by summarizing observations about workforce development programs and identifies gap areas being addressed in the quest to build a stronger cyber workforce.

2 Combating Cyber Workforce Shortage Through Awareness

How is it that a domain exists that has such a profound role in our nation's everyday way of life, and is a key element to our national security posture, but yet has such a drastic shortage of individuals either interested in, or qualified to, defend and protect it? The cyber domain, encompassing all networks and systems ubiquitously connected to provide utilities, services, ecommerce, and entertainment, has exponentially expanded over the past few decades to become the fabric of civilian existence. Communication capabilities run everything in today's homes from coffee makers to automobiles, tell us where we need to be and how to get there, allow instant access to news and messages no matter where we are, faster than it took to draft that message, and manages our finances to the point that most people rarely have the need for physical currency. The conveniences afforded by cyber capabilities are endless, and endlessly relished.

Consider all the ways that some form of technology or cyber capability is used to mitigate risks in several aspects of our lives. To protect our homes, sophisticated monitoring devices that will activate outdoor lighting or alert emergency responders with the trip of an alarm, are used. We put microchips in our pets so that they can be recovered if lost. We use GPS in a multitude of scenarios for tracking and recovering. To restrict access to professional office space, or even our children's daycare centers, it's not the old-school lock and key, it is technology accepting your required means of authentication and maintaining digital records of your comings and goings. Cyber capabilities are crucial components to everyday functionality and used to ensure the preservation of things most valued. Why hasn't the security, ensuring the availability and integrity, of the cyber domain itself rated among the most valued from the populace?

Cyber breaches and vulnerabilities exploited in technologies are regular staples in public news reports. The effects of these breaches have crossed lines of areas of interest, age groups, economic classes, and lifestyles. If one hadn't heard news of the stuxnet attack on nuclear facilities, wasn't cognizant of the theft of financial information from major retailers, then certainly one of the outcomes from the Sony hack should have some familiarity. These cyber breach events are reported from just about every information resource and in every media form. Perhaps some believe these incident reports will be too technical in nature, or do not apply to them as individuals, and hence do not pay much attention. There are however, catchy cyber news links that are aimed at everyman. For example, June 2016, news surfaced of millions of stolen credentials being traded on the dark web. The news links weren't referring to how the records were stolen per se, or how one could search leaked databases and remove their own personal information. The headline links were much more low-level, but equally, if not more important. "The most frequently used password is…", or "Many users still using password as their password", and "123456 passes 12345 as most commonly used password", were just a few of these headlines. These statements should have grabbed the attention of many users as they realized the headlines applied to them, and in turn, accessed the article where they would have learned a valuable lesson on password complexity and using two-factor authentication.

These examples highlight that while it may be believed to be highly publicized that our nation needs to be seriously concerned about cybersecurity and the significant shortage of skilled cybersecurity professionals, this message may not be reaching much further beyond the current cyber workforce.

While addressing this problem, and realizing the criticality of it, is of top priority for government agencies, it cannot solely be their responsibility. Protecting cyberspace from vulnerabilities and attacks has to be a nationwide effort at all levels to have a meaningful impact.

Many awareness initiatives are underway, with varying focus areas, and targeting several audiences. The concentration for the general public is primarily personal information protection and safe computing practices. For school-aged children and young adults, introduction to cyber operations and career fields are additional goals. Awareness efforts for the existing workforce include training and education strategies to effectively develop essential expertise in cyber roles, and retain the talent once cultivated.

2.1 Diversity Efforts

Accompanying the drastic shortage of adept cybersecurity professionals, is a lack of diversity in the existing workforce. As the cyber industry continues to grow and evolve, there are endeavors underway targeting women in order to better diversify the cyber labor pool. According to several studies, women are significantly underrepresented in the field. An (ISC)2 2015 Global Information Security Workforce Study, in which close to 14,000 information security professionals participated, concluded that female representation in the workforce hadn't increased from the 10% reported in the same study, two years earlier.

However, it is important to note that in the growing cyber-related fields of governance, risk, and compliance management (GRC), women are increasing their footprint. Today's cyber issues are more complex, and the needed skillsets have broadened. Advanced technical competencies will always be vital, but there are new demands for roles in the career field which require skills such as problem solving, risk management, and keen business sense. GRC positions depend upon these competencies as well as an ability to encourage collaboration among groups, diffuse emotions, and balance several, many times conflicting, priorities. Panelists in the (ISC)2 study identified emotional intelligence and insightfulness honed through childrearing, as attributes needed for future leaders in the information security profession. These, as well as the aforementioned skillsets and attributes, are typically used to describe characteristics of women. Their increased presence in these GRC roles seem natural, if not essential. The GRC functions play a vital part in shaping the evolution of future practices in information security. Even if women aren't represented in the cyber field by population numbers, the impact they will have through these related leadership positions will ensure they are counted.

Another statistic that has remained constant is that women continue to outnumber men in American colleges. If women are more likely than men to earn a college degree, 30.2% versus 29.9%, according to a 2015 *Time* article quoting census data, then certainly efforts to steer their majors towards technology and engineering should aid in increasing their presence in the cyber workforce. Even more so if awareness of the cyber field as a career choice started much earlier in an individual's education path. According to a 2015 Raytheon millennial survey, 74 percent of young women versus 57 percent of young men, claimed neither their high schools nor secondary schools, provided the skills needed to pursue computer science fields. Also staggering is that 62 percent of all millennial respondents reported that the career field had never been mentioned to them by guidance counselors or teachers. Awareness of cyber security career opportunities and the skillsets required, has to start earlier in schools in order to have growth in the cyber workforce pipeline realized. A rapidly expanding initiative, STEM, may support this cause and encourage changes in current trends.

STEM, or science, technology, engineering, and math fields of study, are subjects that are typically taught in isolation and not part of a curriculum where students would experience how they apply to each other, or real world situations. STEM initiatives were in part created to address the lack of skilled candidates for high-tech jobs, by integrating cyber security into existing STEM curricula, from as early as primary school.

STEM is broadening to STEAM in many K-12 environments. STEAM is the acronym for Science and Technology interpreted through Engineering and the Arts, all based in Mathematical elements. As younger people inherently understand the digital world and are accustomed to and comfortable working with technology, like STEM, STEAM programs integrate the historically separately taught subjects into more of a problem solving, hands-on curriculum more closely aligned with what is experienced in college or the workforce. These programs succeed in reaching both genders, as well as more races and ethnic groups, and at much younger ages. While it will likely take several more years to be able to effectively evaluate how well STEM or STEAM initiatives are helping to increase the number of individuals pursuing cyber careers, or at diversifying the workforce, initial studies appear to support a positive impact.

The first Nations' Report Card for technology and engineering literacy, a study using 21,000 eighth-graders that was released May 2016 from The National Assessment of Educational Progress (NAEP), found that girls performed better than boys with using technology and engineering to solve problems, and had higher average scores overall. For the study, students from around the country were provided computers and internet access, and their capability to evaluate and solve problems was assessed through scenario-type tasks.

The findings illustrating that females performed better than males in this concentration, is supportive reasoning for why girls should be given the same exposure and guidance on cyber careers and the skills required for these careers, as boys are. Targeting eighth-graders for the study was a valuable awareness exercise as the students were given the opportunity to experience technology and engineering in real-life simulated situations, at critical time, right before they enter high school and begin to consider career paths to pursue.

Lack of awareness for children and young adults continues to be one of the major contributors to the slow growth of interest in cyber careers, for both genders. The annual Raytheon millennial cyber survey also reported that interest and awareness are only growing slightly each year. Less than a quarter of the millennial survey respondents indicated they had their first cyber safety discussion from their teacher, less than half were made aware of careers in cybersecurity, and almost three quarters weren't aware of any cyber attacks in the past year. Not only are cybersecurity issues not a primary focus in schools, but they are not part of awareness in newsfeeds, social media sites, or other media streams that are popular with millennials. A good majority are not "getting the memo."

The importance of cybersecurity awareness applies equally to the existing cyber workforce. Awareness efforts don't cease once individuals pursue career fields in technology, or enter the workforce; in fact, it may be more vital. The old familiar saying, “you’re only as strong as your weakest link”, is in no area more applicable than in cyber operations. Humans are the weakest link in cybersecurity and a regular focus at industry gatherings such as the 2015 Cyber Security for Defense conference where keynote speaker, Commander of U.S. Cyber Command, Admiral Michael Rogers, and several speakers to follow, provided examples and data supporting the criticality of user cybersecurity awareness. Admiral Rogers passionately drove home to the audience that users are the first line of defense and that awareness programs and regular refreshers need to be a higher priority.

Bryan Sartin, executive director of global security solutions at Verizon Enterprise Solutions, described the findings of their 2016 Data Breach Report as boiling down to one common theme – the human element. Data from the 2016 report, which analyzed over 2,260 data breaches and 100,000 security incidents from the previous year, shows that user error such as misconfigurations or unpatched systems, lost or stolen devices, mis-handling proprietary information, and social engineering attacks are the root cause for a significant number of the incidents. Complex systems are proving to be less important than the basics, as complex systems can’t prevent user error or bad judgement. A specific social engineering attack, phishing, tops the list of growing concerns. Many organizations are falling victim to this three-pronged attack, and it continues to be reused by cyber adversaries. The user receives an email that appears to be legitimate, but the email contains a link to a malicious website or malware attachment. The user clicks the link or attachment which initiates the download and/or installation of any variety of malware. The adversary then unleashes his bag of tricks such as encrypting system files and demanding ransom to decrypt, or installing keyloggers to capture user credentials and accessing additional systems like the user’s online banking accounts.

Cybersecurity awareness is essential, but it is difficult to universally achieve with confidence. SANS Securing The Human 2016 Security Awareness Report highlighted two major challenges to securing the human, which were revealed through their survey respondents. The first challenge is upper management buy-in. Without executive support, both financial and by decree, an awareness program will not reach the maturity required for meaningful impact.

The other challenge is the lack of what is described as soft skills. Soft skills are the non-technical attributes like communications and human behavior modeling and learning, which are essential for culture change. Most highly technical people are proficient in providing input to computer systems and applications to get desired outcomes. However, they may have difficulty effectively communicating to colleagues or subordinates, tailoring the message for different audiences, and delivering it in a meaningful encouraging way. Technical staff will have to invest in learning these soft skills, or organizations will need to add talented communicators to their cybersecurity efforts even if it means outsourcing this particular expertise.

Factors that are major contributors to the lack of cybersecurity awareness and the slow flow of individuals pursuing cyber careers, are problems that can be fixed. Cybersecurity is an issue that applies to virtually everyone, and the criticalness of online safety should be seen as a priority on individual, local, and global scales. There are many resources that the public, organizations, parents, and educators can utilize to contribute to improving not just the interest and awareness statistics, but ultimately have an impact in improving the nation’s cybersecurity posture.

2.2 Cybersecurity Awareness Resources

A great example of a communal awareness resource is The National Initiative for Cybersecurity Education (NICE). NICE is a coordinated effort between federal agencies, industry, and academia, led by the National Institute of Standards and Technology (NIST). NICE was established in response to the Comprehensive National Cybersecurity Initiative (CNCI), a set of initiatives published in 2008 that were created to help secure the United States in cyberspace (specifically, CNCI Initiative 8 calls for the need to expand cyber education, awareness, and professional development).

NICE has three goals and three target audiences: to raise the general public's awareness of the risks in cyberspace; to broaden the pool of prepared cybersecurity workforce members and focuses on students; and to cultivate a globally competitive cybersecurity workforce through standards and strategies for recruitment, training, and retention. These three goals are organized under components, each led by one or more federal agencies, and have defined objectives and strategies for meeting those goals.

The NICE website not only serves as a central location for current cybersecurity newsworthy events, new federal and state level programs, and other mission related features, the component areas contain numerous goal focused resources. For instance, the education component lead by the Department of Education and National Science Foundation, has several activities and information aimed at boosting cybersecurity education programs. Visitors to this area of the site may access a plethora of guidance on cyber education programs or existing educational materials that may be utilized for their training needs.

The awareness component of NICE is led by the U.S. Department of Homeland Security (DHS). Besides DHS' participation in the NICE initiative by taking charge of awareness with its wealth of available materials for their *Stop.Think.Connect.* campaign, and establishment of National Cyber Security Awareness Month, the agency has another web portal bursting with information and publically available resources. The National Initiative for Cybersecurity Careers and Studies (NICCS), is touted as the *One Stop Shop for Cybersecurity Careers and Studies*. Their NICCS portal has goals in common with NICE by aiming to make the general public keen on safe computing and cybersecurity issues, sharpening the skills of the existing cyber workforce, and increasing the pipeline of future qualified cybersecurity professionals.

From reporting or researching cyber incidents, to investigating cyber careers or insurance, to obtaining awareness material or guidance on training plans, the DHS site has information to readily assist, and additional resources. DHS recognizes its mission within the cyber domain is one that requires cooperation and coordination from every sector, and offers tools to help achieve this mission.

As imperative as cybersecurity awareness is to all audiences, the evidence that it is not a priority, or even a consideration, in many circles is concerning. The resources, tools, and guidance are plentiful and readily available; the application and appreciation just need a boost. Encouraging safe computing and awareness for school-aged children could be carried out through games and activities available from sources like NetSmartz or Cyber Surf Islands. NetSmartz from the National Center for Missing & Exploited Children, and Cyber Surf Islands from the FBI, are resources for interactive games and tools, available for different ages, as a fun and engaging way to teach the younger generation online safety. With children using technology at younger ages at home and in classrooms, cyber awareness is likely to become more prevalent. Parents' interest in their children's cyber activities, coupled with their own technology experiences, and regular news reports of data theft, digital privacy invasions, or other cyber-related compromises, should surely help lead to a natural progression of stronger cyber awareness for the public.

The obstacles that organizations face preventing successful awareness programs and the formation of a more cybersecurity-conscience culture, are ones that can be resolved. As the SANS Security Awareness Report reveals, management support by ensuring budget, time, and proper communication resources, as well as endorsing policies, are essential components to meaningful security awareness programs. If technology is not a part of an entity's primary mission, or there is a lack of in-house staff with the communication talents needed to achieve user buy-in, there are numerous outsourcing options to manage an awareness program. Specific to organizational goals and needs, awareness programs include regular refresher training, and compliance checks that may invoke additional training or other corrective action for areas of weakness. Example compliance checks are: quizzes reflecting the lesson material; social engineering penetration tests (such as impromptu inspections of discarded material for potential data compromise); attempts to gain unauthorized entry into restricted areas; and sending phishing emails to test if users will take the bait.

There is great value and insight gained from these compliance validations. First and foremost, they give organizations a sense of the strength of the human element of their security posture, and identify areas for improvement. Second, if users know sound security practices are highly valued and being monitored, they are more likely to be thoughtful and deliberate with their actions. Also, if the results of the compliance checks are made known to users, it encourages active participation by including them in an important cause where they are able to relate security practices to their specific duties.

Cybersecurity awareness is a critical piece to cyber workforce development. Awareness of the career field itself to help increase the number of people pursuing careers in technology and address the shortage of skilled professionals needed to fill the numerous open positions. Also, awareness of threats and safe computing best practices to strengthen the operational preparedness of current and future cyber professionals, and reverse current trends of compromise through human error.

3 Training Initiatives

Cybersecurity awareness is an essential part of baseline training for the cyber workforce. From there, the cyber field branches out into many specialty and sub-specialty concentrations that each require their own unique training focus. Similar to medical and legal occupational fields, there are foundations to understand before progressing into the development of expertise within an area of practice. Identifying appropriate training for each cyber-related concentration and mechanisms to qualify skill proficiency within the multi-faceted workforce, are on-going efforts. Organizations, government agencies, and other entities have executed training programs, initiatives, or directives, aiming to cultivate a highly skilled workforce that is prepared to protect and defend in the cyber domain.

3.1 National Cybersecurity Workforce Framework

While the National Cybersecurity Workforce Framework isn't a training initiative per se, it is a guiding force, or foundation, for several training programs and cyber workforce development endeavors. The framework, a national resource originally published in 2012 by NICE, and recently updated with DHS' lead, addresses the need for standard terminology and identification of cyber workforce position descriptions, and required knowledge, skills, and abilities (KSAs) for tasking performed as part of specific cyber job roles.

Within the framework, categories and specialty areas are used to organize and group similar types of work. Categories serve as an overarching structure for the framework and group related specialty areas together. Each specialty area contains common tasks and KSAs. The framework is designed to define cybersecurity work regardless of organizational structure and to be flexible enough to allow entities to adapt to fit their workforce-planning needs. The latest update to the framework incorporated input from government agencies, academia, and the private sector to better identify the full spectrum of cyber operations and responsibilities.

The framework will help with the establishment of standards and guidance for cybersecurity training and professional development. As focused, targeted training is necessary to ensure the cyber workforce has the appropriate competencies needed to fulfill cyber work roles, training that aligns with the specialty areas in the NICE framework will be mapped or otherwise endorsed. The framework may also help identify gaps between specialty area needs and training opportunities. A void in effective training for a specialty area could highlight weaknesses in cyber workforce readiness. The framework strives to be comprehensive in its inclusion of cyber work roles as well as customizable enough to be adapted into any organization, and is likely to be the standard blueprint for cyber workforce definition and building of training plans.

3.2 CYBERCOM Joint Cyberspace Training & Certification Standards (JCT&CS)

USCYBERCOM directed its training and development efforts through the Joint Cyberspace Training & Certification Standards (JCT&CS) Initiative. The JCT&CS was the first joint cyber training framework of its kind. It was designed to be continuous, growing, and adapting as technologies and tactics evolve.

The joint training and certification standards developed by the JCT&CS are in the operational context and mission requirements of CYBERCOM and its components. Training standards are defined for each job role and for collective audiences. The procedures for implementing the initiative are patterned after the Joint Training System's (JTS) four phases of requirements, planning, execution, and assessment. Commanders have integrated processes used to evaluate the command's missions and determine the tasks that are essential to accomplishing those missions. These processes were designed to improve the commander's joint readiness by linking plans, training, and assessments to mission requirements.

A prioritized list of essential tasks, their conditions, and measurable standards required to complete a mission is created and known as the Joint Mission Essential Task List (JMETL). The JMETL helps to form the answer to the question of mission readiness: To complete this mission, this organization must accomplish these tasks under these conditions to meet these standards. Training plans that include audiences, objectives, and methods are formed based on the requirements defined in the JMETL, as well as baseline standards that are derived from tasks and skill sets identified within cyber work roles. Feedback is collected throughout the training and assessment phases and used as input for planning the next training cycle.

This initiative for their workforce is driven by specific missions, the operations required to complete a specific mission, and measures of success for mission achievement. The design of this model is very similar to the goals of the NICE Cybersecurity Workforce Framework. The JCT&CS identified work roles with baseline training, mission essential tasks, and measurable standards for success. Similarities between the JCT&CS and the NICE framework can be seen with missions or specialty areas of work, and accompanying tasks and KSAs.

3.3 Department of Defense (DoD) Directive 8570.01 Information Assurance Training, Certification, and Workforce Management

One of the first cyber workforce training initiatives established is the Department of Defense *(DoD) Directive 8570.01 Information Assurance Training, Certification, and Workforce Management* initiative. This initiative is designed to provide the basis for an enterprise-wide solution to train, qualify, and manage the DoD Information Assurance (IA) workforce. The directive calls for information assurance technicians (IAT) and managers (IAM) to be trained and qualified at a baseline requirement. The policy applies to all organizational entities in the DoD performing IA functions.

The manual that provides guidance and procedures for supporting the directive, DoD 8570.01 *M*, was approved in December 2005. The latest version, Change 3, was published in January 2012. The directive addresses workforce management issues by calling for IA positions to be identified and documented, and for qualified personnel to be accounted and assigned to those positions.

To reach this goal, all IA positions are categorized as technical (IAT), management (IAM), system architecture and engineering (IASAE), or computer network defender service provider (CND SP) and are assigned a level or specialty within each category. Individuals must obtain an approved certification from a category to be qualified for a corresponding position. Change 3 specifies that all personnel who perform IA functions must obtain a baseline and computing environment certification and/or certificate of training within six months of being hired in an IA position.

The goal of *DoD 8570.01* was to build an IA workforce with the knowledge and skills to protect and defend DoD systems and information assets in cyberspace. The right people, with the right skills, in the right position. The office of the DoD Chief Information Officer (CIO) validates, monitors, and reports on the certification status of IA workforce members through the Defense Workforce Certification Application (DWCA) database.

3.4 Department of Defense (DoD) Directive 8140 Cyberspace Workforce Management Policy Update

DoD 8140 Cyberspace Workforce Management Policy Update reissues and renumbers *DoD 8570*. Effective August 11, 2015, *DoD 8140* supersedes the 8570. However, the manual for the 8140 containing the details for the new directive, is still being written. Until the 8140 manual is finalized, the 8140 directive will assume the 8570 manual, 8570.01-M. Individuals will need to comply with the 8570.01-M manual and obtain industry certifications as mandated, under the 8140 directive.

The 8140 directive is expected to be more versatile and comprehensive. It is driven by the NICE Cybersecurity Workforce Framework, which as described previously, aims to help with consistency when defining jobs roles within cyber operations through 32 cyber specialty areas categorized into seven high-level areas of operations. The 8140 offers more granularity for categorizing the DoD cyber workforce, enables a clearer picture of workforce strengths and gap areas, and helps guide training plans to specific task goals.

The requirement for cyber professionals to obtain an approved industry certification is not expected to go away. However, a certification alone will no longer be enough to validate an individual’s qualifications. Employers will be looking for a certification plus a credential that asserts the individual achieved expectations in a skill-specific training and assessment program from an approved training source.

In support of the 8140 and the need for consistency with defining cyber operations work roles, the DoD Chief Information Officer worked with representatives from several DoD components to develop the DoD Cyberspace Workforce Framework (DCWF). The DCWF takes the structure and definition guidance of the NICE Cybersecurity Framework and incorporates mission essential tasks and KSAs from the Joint Cyberspace Training and Certification Standards (JCT&CS) to identify a gamut of cyber workforce roles.

The DCWF is intended to be reviewed regularly and updated as DoD missions, directives, and cyber operations evolve. Additional supporting information identifying specific qualification requirements and credentials for specific work roles, is expected.

The Office of Personnel Management (OPM) issued codes corresponding to these categories, and DoD codes for each specialty area. The codes are used uniformly to catalog the cyber workforce, their area of work and specific specialty, within training and certification tracking databases such as the Army Training and Certification Tracking System (ATCTS).

These systems could prove to be valuable tools by helping to determine baseline capabilities, evaluate workforce demands, identify training gaps, and aid in effective and targeted recruitment and retention of a skilled workforce.

A supporting tool of the 8570/8140 directive is the Federal Virtual Training Environment (FedVTE). FedVTE is an online training and learning management system sponsored and managed by DHS. As of June 2016, FedVTE serves over one hundred thousand users from federal, state, and local government agencies, with thousands of hours of cybersecurity and certification prep training materials, accessed 24 hours a day, seven days a week. This system saves millions of dollars in travel and training costs because users can access courseware free of charge from anywhere in the world.

Course completion certificates from FedVTE are accepted by industry certification agencies for continuing education credits which are required to maintain a certification after an individual has passed the certification exam. While the training within FedVTE assists with preparing for a certification exam as well as maintaining the certification post exam, the system is also valuable for supporting anticipated 8140 goals of training related to specific job roles, through its growing catalog of cybersecurity related materials.

3.5 DISA Cyberworkforce Development Initiatives

DISA, the Defense Information Systems Agency, is a major contributor and pioneer of new capabilities to support cyber workforce development. As the agency’s responsibilities include defensive cyber tactics on a national level including commanding and controlling the Department of Defense Information Network (DODIN), and providing defensive cyberspace and IT combat support for the DoD, they have an emphasized focus on advanced cyber capabilities and ensuring operators have the skills, tools, and resources necessary for mission success. They are budgeted to support the IT needs and requirements of the entire Defense Department and as such, make cyber workforce development content available across the DoD.

DISA is actively creating a workforce training and assessment program that is modeled after the previously mentioned DoD Cyberspace Workforce Framework (DCWF). They identified unique cyber roles performed within DISA which have corresponding KSAs and proficiency level, to which training plans and assessments will be established. The assessments will be designed to evaluate increased competency for individual and collective tasks and aid in measuring cyber readiness. Using the DCWF, DISA coded their entire workforce at specialty and role levels which created valuable data for manpower tracking and analyzing qualifications and additional needs.

Curriculum that is developed for specific roles and proficiency levels is published on their Information Assurance Support website and is accessible by DoD personnel. Making these resources available not only saves other components money and effort by not having to create their own custom role training, it helps with standardizing definitions and expertise metrics for role and tasks operations within the cyber workforce.

DISA has other initiatives such as the DoD Cybersecurity Range which is a realistic cyber environment that is configurable according to training or testing needs. DISA is leading the evolution of DoD cyber workforce training and skill building. Their efforts towards achieving their cyber operations missions will play a key role in shaping the entire cyber workforce.

3.6 CERT Approach to Cybersecurity Workforce Development

The CERT Division of the Carnegie Mellon® Software Engineering Institute (SEI), a federally funded research and development center sponsored by the U.S. Department of Defense, subscribes to workforce development divided into continuous phases of development. These phases progressively build an individual's knowledge, skills, and experience in ways that are relevant to his or her job duties. Three main phases are followed by a fourth evaluation phase to assess the individual's comprehension of the training.

Phase 1, knowledge building, focuses on teaching fundamental skills and concepts to the learner through online instruction which is more desirable due to cost-effectiveness, time efficiency, and ability to target a desired discipline.

Phase 2, skill building, reinforces concepts learned in the previous phase through task-focused, hands-on exercises. This phase is an integral part of professional development because individuals transform knowledge into the ability to apply it. These exercises focus on an individual skill and take place in a controlled environment free of distractions. Once individuals have accomplished those exercises, they can further refine their skills in the experience-building phase.

Phase 3, experience building, refines the knowledge and skills by applying them to real-world, on-the-job scenarios that lead to maximizing the individual's job performance. No longer in a controlled environment, these scenarios force individuals to successfully operate with additional complexities and unfamiliarity.

Phase 4, the evaluation phase, assesses the knowledge comprehension and skill proficiency achieved through the training. The assessment helps to determine the next training cycle for the individual and serves as a mechanism for organizations to better understand the workforce's strengths and additional training needs.

The CERT Division's approach using continuous phases of development progressively builds an individual's ability and leverages online platforms for knowledge, skills, and experience building. In the end, the approach offers organizations a comprehensive, targeted, and cost-effective training option that can be tailored to their needs [Hammerstein 2010].

® Carnegie Mellon is a registered trademark of Carnegie Mellon University.

4 Evolving Cyber Workforce Training Models

As models for identifying the cyber workforce and the operations they perform continue to become more specific and granularly defined, so will the training tools and accompanying assessment capabilities, in order to have confidence in workforce preparedness. Early cyber workforce training directives served their purpose as the foundation and inspiration highlighting the need to have standardization in this new and rapidly evolving field. However, it became quickly apparent that the field couldn't be painted with such a wide brush, or fit into a few large buckets. An industry certification, plus a training completion certificate from an operating system course, may have formerly been acceptable criteria to indicate an individual was qualified in their categorized work role, but moving forward that will not be sufficient.

While certifications will continue to be valuable indicators of focused strengths, especially those that are advanced and in specialized concentrations, many will not be able to stand alone as skill indicators. The general, high-level certifications that touch on security under a wide umbrella of technical topics can be beneficial to gaging awareness and comprehension. However, with the multitude of "boot camps" to prepare individuals for certification exams, it is difficult to measure whether an individual crammed to pass a test, versus gained an understanding of the concepts covered on the test. This is not to say that some certification exams are easy to pass; they are not. Many senior cyber professionals would need time to brush up in a few areas before sitting for an exam. The downfall of studying for the purpose of obtaining a certification credential is that if the individual doesn't regularly experience and exercise concepts covered within the exam, the knowledge is not likely to be retained long term. German psychologist Hermann Ebbinghaus introduced the Forgetting Curve in 1885. His research found that information is exponentially forgotten, newly learned knowledge halved in a matter of days, unless there is conscience review of the learned material.

An effort to address this was made through requirements that must be met in order to maintain a certification once passing the exam. Requirements to demonstrate actively staying current in a certification field of discipline, also referred to as continuing education, includes activities such as annual hours of related training, re-testing, publishing, or attending or speaking at a conference. Even when an individual has a certification in good standing and participated in several continuing education activities, does that definitively indicate that the individual is proficient in their job role? The answer is probably not.

The Certified Information Systems Security Professional credential (CISSP) is one of the more popular industry certifications due to the breadth of technical content it covers, and experience or education that is required in order to take the exam. Having the CISSP designation after one's name indicating that they have achieved the (ISC)^2 CISSP credential, is frequently used as a symbol of expertise and qualifier for employment. Many open positions in the technology field include CISSP as a preference or requirement within the job description. In June 2016, Indeed.com contained 12,920 employment opportunities with CISSP as part of the description.

As of March 2016, there were 105,816 certified CISSPs globally with 69,130 of those within the U.S. The United Kingdom and Canada follow with 5,402 and 4,577, respectively. The remaining countries trail with less than half the numbers that the U.K. and Canada have. The U.S. has 65% of the CISSPs globally with the next closest country barely having 5%. Countries outside the U.S. appear to have their own strategy for developing cyber expertise within their workforce, and are not subscribing to a global, industry certification.

The certification is a good baseline for cybersecurity professionals, but when the field branches off into niches and subspecialties, the broader certifications will not apply. Again, there are several advanced, specialty certifications available, and no doubt many more in development, but how much of cyber workforce will these apply to? Specialty certifications require years of experience within a discipline. With the high-turnover, whether due to advancement or reassignment within government entities, many will not have time, opportunity, or training budget to pursue an advanced certification. These are some of the considerations that are driving the rapid movement towards role-based curriculums with task-specific skill building and performance based assessments.

Processes and procedures for cyber operations are likely to differ between organizations, however the DoD has been working to consistently define the roles that make up the cyber workforce, and develop standards for training. Regardless of agency, individuals that are identified as performing identical job roles at the same proficiency level, are expected to be trained to a standard where they possess the necessary skills to complete their mission. Baseline cybersecurity and awareness training for all cyber operator roles, plus additional focused task-specific skill building, for individuals and team or tool interactions, with assessment components is where the field is rapidly migrating towards. With organizations and government agencies collaborating on definitions and foundational models, and sharing training and assessment principles, the goal of one standard and the ability to determine individual and workforce preparedness is in sight.

Preparedness is determined through competency to successfully complete a mission to a certain standard, and under a specific set of conditions. As cyber workforce roles are more conclusively defined where every task performed within the many roles have the type and level of skills needed to complete those tasks documented, a collective and swift movement towards skill enhancement and competency evaluation tools will occur.

Competency-based training is not a new concept. Western Governors University was designed in 1995 by 19 U.S governors who wanted to change the way higher education institutions traditionally educated. WGU offers competency-based degrees and credentials leveraging technology to create a flexible way to learn real-world, job-related skills. Success in their programs is determined by proving competence, not completed credit hours. Many of their degree programs require earning industry certifications, and also use other external assessments to evaluate student proficiency, prior to graduation. WGU, an online, accredited, comparably low-cost university that has been endorsed by President Obama and Bill Gates among others, has 65,262 alumni as of June 2016. The competency-based institution not only ranked above average in national studies comparing student engagement and work place well-being after graduation, but 100% of the 305 employers of WGU graduates surveyed in 2015 responded that their graduates were prepared to do their job. This institutional success story illustrates the value of education based on competency of career-required skills.

Skill development and enhancement can be achieved through smaller, focused instructional assets that are concentrated on specific KSAs and customized to operational needs. Organizations will have the ability to prepare workforce members for specific operational duties more quickly, and develop talent using training plans that are structured around required competencies. Research on adult learning retention asserts that lessons that are practical and applicable to the learner and their goal, taught in smaller chunks, and in spaced out repetition, is key to making learning stick, according to findings summarized by Mindflash in June 2016.

Precise skill-based training for user tasking that includes exercise components for demonstrating ability, and performance assessment indicator to determine competency and provide corrective feedback, fits into this model for information retention. The repetition component would ideally be realized through work role operations and experienced in different contexts through team and tool interactions.

As highlighted earlier, the human element of cyber operations is the weakest link in security postures due to error and oversight. Awareness training and education programs would certainly benefit from lesson materials that are designed to be repetitious but spaced out, presented in a context relatable to the audience, and engaging to attract user attention. All the necessary ingredients for creating longer-lasting memories.

One approach to engaging training that is gaining speed in the cyber field is gamification. Gaming options with brief tests provides an entertaining way of learning that also aids in memory retention. This concept has recently been proven effective in other industries. Retail giant Walmart began using a game application to reinforce safety training in 2012. They were looking to solve the problem of employees not having sufficient time for safety procedure training and education. During their pilot program over six months where 5,000 employees used the gaming application for safety training, they saw a 54% decrease in incidents. The retailer has since expanded the training through gaming program include 75,000 employees and additional operational functions.

The DoD has experienced success with game-based training for individual, and team, battlefield tactic training. From as early as 1962, the DoD has sponsored research and development for game-like simulated scenarios that provide realistic experiences with weapons, procedures, team tactics, and the need for critical, timely decision making. The virtual combat gaming environments allowed mistakes to be made and lessons learned, without the costly consequences those mistakes would have on an actual battlefield. A tactical shooter game, America’s Army, originally released in 2002 as a recruitment tool, was not only successful in recruitment, but provided recruits valuable insight through the virtual environment, on what to expect before arriving to basic training. [Allen 2014]

Gamification of training is a successful model because it solves many of the problems or shortcomings that have plagued traditional training programs. Gaming is relatable to all ages and genders. Even if one was not a gamer under the historic definition of sitting in front of a television using a game console for hours, our age of smart phones and portable devices puts video challenge applications of some form, in everyone’s hands. Gaming applications for training addresses the complications of limited time availability, and rapid employee turnover. The games and end-game results are designed to be short, impactful lessons with performance feedback. That design lends to solving user knowledge retention concerns. As mentioned, retention is best achieved through small, relatable, repeatable lessons. The object of most games is to successfully complete a level and continue to progress through more difficult stages leveraging the skills that were required to achieve the previous stage. This is very relatable and applicable to competency building.

Cyber security awareness training through gaming has already taken off. The community searching for more effective ways to secure the human element has inspired this movement. Black Hat, which is known as a very technical security event that attracts pioneers and experts in the cyber field, has a briefing planned for their summer 2016 conference which will detail how to conduct awareness training through playing a game. The game is aimed at what the author describes as the neophyte audience, those who are bored or scared by existing security training. The role playing game will take users through attacking and defending a building. At the completion of this real-world modeled threat gaming scenario, the debrief will link the similarities between the game and security stakes. Analogizing real-world situations to cyber security is one of the many types of games and gaming goals.

There are several resources where games are used to educate and better relate to younger children and teens. This generation that is by far more technical and fully immersed in the digital world at a younger age will likely need games and catchy graphics to be inspired and engaged. Besides cyber safety topic games such as those available from NetSmartz and Cyber Surf Islands, STEM curriculum gaming is available for subjects taught using, and leveraged by, technology. NOVA Labs is a free online platform where teens perform authentic scientific exploration through investigations analyzing the same data scientists use.

The gamification of industry training is looking to be the way of the future. As simulated environments to exercise realistic hands-on cyber operations have been viewed by many as an effective skill and expertise building model, the transition to similar gaming applications for cyber workforce functions seems like a natural progression.

5 Conclusion

The nation’s cyber workforce is lacking in numbers and in talented individuals needed to effectively operate in cyberspace. Every sector of the nation operating in cyberspace is cognizant of the threats in this domain and the lack of enough people resources, or “human capital,” who are adequately prepared to defend and protect critical systems and services. Threats in the form of incidental human or equipment error, or attacks launched with an end goal of service disruption, financial gain, espionage, or annoyance, are evolving in number and sophistication. The cyber workforce must mature in turn.

Cyber workforce development efforts are in part focused on growing the number of information security professionals in the workforce, as well as enhancing the operational abilities of those already counted in the workforce. There are two major contributors to the shortage of available qualified professionals to adequately staff and operate within the cyber workforce; lack of awareness and qualifications.

Cybersecurity awareness efforts to attract more viable candidates to join the workforce have initiatives for reaching individuals of all ages and technical backgrounds. Campaigns with catchy slogans, videos and activities for children and teens, strategic insertion of concepts into K-12 curriculum, even an entire month designated nationally as Cyber Security Awareness Month, are just a few of these efforts. Unfortunately, the message of the opportunities within the cyber field and the importance of the work, either hasn’t reached, or hasn’t interested, enough people to make a significant difference in the growth of the workforce population or those pursuing it as a career path.

Determining individuals’ skill proficiency, required competencies for work roles, and corresponding effective training to ensure operational preparedness, is a gap area in the existing cyber field. Several cyber workforce training directives have been created to support cyber workforce development and training. There have been major strides in community collaboration efforts leading to common goals and new strategies to achieve them. All government and military personnel performing cyber duties, as well as many industry and academia cyber professionals, are adhering to similar initiatives either by mandate or as a best practice. This is leading the way to standardization of definitions and training.

Universal descriptions of cyber work roles and the tasks performed within each role, will guide the desire for training that is more laser focused on skill proficiency building and include mechanisms to assess competency. Knowledge retention is most effective when the training is in smaller pieces that are relatable to the learner, and repetitious. Learning through small lessons that evaluate comprehension and provide feedback that can be applied to future lessons experienced through a different context, is an example of a proficiency building model.

Game-based training is an effective model for cybersecurity training and skill building. Gaming allows learners to be engaged in cyber operations within simulated real-world scenarios to practice techniques without having consequences of their decisions affecting production systems or networks. Graphically-appealing, user-action driven applications appeal to all ages and genders, and meet the conditions for effective knowledge retention.

Effective cyber workforce development is attainable. As awareness efforts continue to expand far and wide to reach more audiences, and technology continues to be involved in most aspects of everyday life, interest in cyber-related fields is bound to increase, and the pipeline of those pursuing cyber careers will flow smoothly. Those entering the cyber workforce will be deemed qualified and better prepared to protect and defend in cyberspace because of fully defined workforce roles and training plans based on individual skill building and competencies.

References

URLs are valid as of the publication date of this document.

[Aldridge 2010]
Aldridge, Susan & Raduege, Harry Jr**.** *Build an Army of Cyber Warriors.* http://articles.baltimoresun.com/2010-08-30/news/bs--ed-cyber-soldiers-20100830_1_cyber-security-cyber-warriors-cyber-threat

[Allen 2015]
Allen, Dennis & Herr, Christopher. *Video Games as a Training Tool to Prepare the Next Generation of Cyber Warriors.* http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=442338

[Cisco 2015]
Mitigating the Cybersecurity Skills Shortage *Top Insight and Actions from Cisco Security Advisory Services*. http://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf

[CNN Money 2016]
Goldman, David. 123456 is the most common password in a massive Twitter heist http://money.cnn.com/2016/06/09/technology/twitter-password-common-heist/

[CyberCityUSA.org 2013]
CyberCityUSA.org. *CyberCityUSA San Antonio, Texas homepage.* http://cybercityusa.org/home (2013).

[DoD 2012]
U.S. Department of Defense. *DoD 8570.01-M, Information Assurance Workforce Improvement Program*. DoD, January 24, 2012.

[Forbes/Tech 2016]
Morgan, Steve (contributor). *Calling All Women: The Cybersecurity Field Needs You And There's A Million Jobs Waiting.* http://www.forbes.com/sites/stevemorgan/2016/03/28/calling-all-women-the-cybersecurity-field-needs-you/#5d59a84f5ca4

[Hamill 2013]
Hamill, Jasper. "Verizon: 96 PER CENT of State-Backed Cyber-Spying Traced to China." *The Register*. http://www.theregister.co.uk/2013/04/23/spies_verizon_security/ (April 23, 2013).

[Hammerstein 2010]
Hammerstein, Josh & May, Christopher. *The CERT Approach to Cybersecurity Workforce Development* (CMU/SEI-2010-TR-045). Software Engineering Institute, Carnegie Mellon University, 2010. http://www.sei.cmu.edu/library/abstracts/reports/10tr045.cfm

[Homeland Security Advisory Council 2012]
Homeland Security Advisory Council. *CyberSkills Task Force Report, Fall 2012*. U.S. Department of Homeland Security, 2012. https://www.hsdl.org/?view&did=723343

[indeed 2016]

Cissp jobs. www.indeed.com/q-Cissp-jobs.html

[(ISC)^2 2016]
Inspiring a Safe and Secure Cyber World. (ISC)^2 Member Counts CISSP listing. https://www.isc2.org/member-counts.aspx

[(ISC)^2 Foundation 2016]
A Frost & Sullivan White Paper. *Women in Security: Wisely Positioned for the Future of InfoSec* https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/2015-Women-In-Security-Study.pdf

[Kay 2012]
Kay, David J.; Pudas, Terry J.; & Young, Brett. "Preparing the Pipeline: The U.S. Cyber Workforce for the Future." *Defense Horizons 72* (August, 2012).
http://www.ndu.edu/CTNSP/docUploaded/DH%2072%20for%20web.pdf

[Mindflash 2016]
Repetative spaced out learning: making Learning Stick.
https://www.mindflash.com/blog/repetitive-spaced-learning-making-learning-stick/

[NAEP 2016]
National Assessment of Education Progress. Lestch, Corinne. *Girls outperform boys in tech and engineering literacy in new study*.
http://edscoop.com/girls-outperform-boys-in-tech-engineering-literacy-according-to-nations-report-card

[NICCS 2016]
National initiative for cybersecurity careers and studies. *The Need for Women and Minorities in Cybersecurity*. https://niccs.us-cert.gov/home/women-minorities

[PR Newswire 2014]
Latest Raytheon research on millennials finds rising interest in cybersecurity careers *Report finds high schools not addressing student interest and employer demand as National Cyber Security Month begins*. http://www.prnewswire.com/news-releases/latest-raytheon-research-on-millennials-finds-rising-interest-in-cybersecurity-careers-277724161.html

[PR Newsire 2016]
Verizon's 2016 Data Breach Investigations Report finds cybercriminals are exploiting human nature. http://www.prnewswire.com/news-releases/verizons-2016-data-breach-investigations-report-finds-cybercriminals-are-exploiting-human-nature-300258134.html

[Raytheon 2015]
NOW HIRING: CYBER DEFENDERS NEEDED A new survey details the growing talent gap in cybersecurity. 74% of women 57% of men didn't get skills in school. Raytheon
http://www.raytheon.com/news/feature/now_hiring.html

[Roman 2012]
Roman, Jeffrey. *Scholarship for Service Opportunities: SFS Program Director Offers Advice for Students*. http://www.careersinfosecurity.com/scholarship-for-service-opportunities-a-4616/op-1 (March 23, 2012).

[STEAM 2016]
What STEAM stands for
http://steamedu.com/about-us/

[TB&P 2014]
Souza, Kim Talk Business & Politics The City Wire. *Gaming software helps Walmart logistics improve safety education, culture*. http://talkbusiness.net/2014/03/gaming-software-helps-walmart-logistics-improve-safety-education-culture/

[The Washington Post 2014]

Anderson, Nick. *The gender factor in college admissions: Do men or women have an edge?* Women outnumber men in American colleges. https://www.washingtonpost.com/local/education/the-gender-factor-in-college-admissions/2014/03/26/4996e988-b4e6-11e3-8020-b2d790b3c9e1_story.html

[TIME 2015]
Feeney, Nolan. *Women Are Now More Likely to Have College Degree Than Men.* 30.2% women have degrees to 29% men. http://time.com/4064665/women-college-degree/

[USCC 2010]
United States Cyber Command (USCC). *U.S. Cyber Command Concept of Operations*. http://itlaw.wikia.com/wiki/U.S._Cyber_Command_Concept_of_Operations (2010).

[WGU 2016]

Western Governors University. http://www.wgu.edu/about_WGU/overview

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412/268.5800 | 888.201.4479
Web: www.sei.cmu.edu | www.cert.org
Email: info@sei.cmu.edu

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Department of Homeland Security or the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM-0003988