Developing Your

Cybersecurity Career:

Resources for Students

Edited by

Michael Erbschloe

Connect with Michael on LinkedIn

Table of Contents

Section	Page Number
About the Editor	3
Introduction	4
The National Cybersecurity Workforce Framework	7
Finding Where Jobs are Located	15
College Education for Cyber Operations Careers	17
College Education for Cyber Defense Careers	47
NSA/DHS National Centers of Academic Excellence for Cyber Defense Focus Areas	49
NSA/DHS National Centers of Academic Excellence in Cyber Defense (CD) Knowledge Units	65
NSA/DHS National CAE in Cyber Defense Designated Institutions	92
National Initiative for Cybersecurity Careers and Studies Education and Training Catalog	113
Cybersecurity Professional Certifications	114
Cybersecurity Job Descriptions	117
References	139

About the Editor

Michael Erbschloe has worked for over 30 years performing analysis of the economics of information technology, public policy relating to technology, and utilizing technology in reengineering organization processes. He has authored several books on social and management issues of information technology that were published by McGraw Hill and other major publishers. He has also taught at several universities and developed technology-related curriculum. His career has focused on several interrelated areas:

- Technology strategy, analysis, and forecasting
- Teaching and curriculum development
- Writing books and articles
- Publishing and editing
- Public policy analysis and program evaluation

Books by Michael Erbschloe

Social Media Warfare: Equal Weapons for All (Auerbach Publications)
Walling Out the Insiders: Controlling Access to Improve Organizational Security (Auerbach Publications)
Physical Security for IT (Elsevier Science)
Trojans, Worms, and Spyware (Butterworth-Heinemann)
Implementing Homeland Security in Enterprise IT (Digital Press)
Guide to Disaster Recovery (Course Technology)
Socially Responsible IT Management (Digital Press)
Information Warfare: How to Survive Cyber Attacks (McGraw Hill)
The Executive's Guide to Privacy Management (McGraw Hill)
Net Privacy: A Guide to Developing & Implementing an e-business Privacy Plan (McGraw Hill)

Introduction

> *Cybersecurity is the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.*

There is no doubt that there is a great need for well trained professionals working in cybersecurity roles. These professionals are critical in both private industry and the government for the security of individuals and the nation. The U.S. Government is committed to strengthening the nation’s cybersecurity workforce through standardizing roles and helping to ensure we have well-trained cybersecurity workers today as well as a strong pipeline of future cybersecurity leaders of tomorrow.

Starting with the country’s youngest students, DHS has partnered with not-for profits, middle and high schools, Universities, and State school boards across the country to help incorporate cybersecurity concepts into classrooms. For the past several years, DHS has partnered with the National Integrated Cyber Education Research Center (NICERC), a not-for profit academic development center to provide K-12 cybersecurity curricula and hands-on professional development for teachers at no cost. The grant has helped get cybersecurity curricula into the hands of over 15,000 teachers impacting 820,000 students in 42 States. Individual states can work with DHS and NICERC to approve the curricula state-wide.

As high priority has been strengthening cybersecurity by creating higher education to programs to produce skilled and capable cybersecurity. DHS and The National Security Agency (NSA) jointly sponsor the National Centers of Academic Excellence (CAE) program, designating specific 2- and 4-year colleges and universities as top schools in Cyber Defense (CD). Schools are designated based on their robust degree programs and close alignment to specific cybersecurity-related knowledge units (KUs), validated by top subject matter experts in the field. CAE graduates help protect national security information systems, commercial networks, and critical information infrastructure in the private and public sectors.

To encourage students to enter cybersecurity degree programs, DHS co-sponsors the CyberCorps®: Scholarship for Service (SFS)— providing scholarships for bachelors, masters, and graduate degree programs focusing in cybersecurity in return for service in Federal, State, local, or tribal governments upon graduation. The scholarship assists in funding the typical costs incurred by full-time students while attending a participating institution, including tuition and education and related fees. The scholarships are funded through grants awarded by the National Science Foundation (NSF) in partnership with DHS and the Office of Personnel Management (OPM).

The National Cybersecurity Workforce Framework is the foundation for increasing the size and capability of the U.S. cybersecurity workforce. It is a national resource that categorizes, organizes, and describes cybersecurity work. The National Cybersecurity Workforce Framework provides educators, students, employers, employees, training providers and policy makers with a system for organizing the way we think and talk about cybersecurity work, and what is required of the cybersecurity workforce.

Additionally, DHS's National Initiative for Cybersecurity Careers and Studies (NICCS) serves as a national resource for cybersecurity awareness, education, training, and career opportunities. NICCS makes research and training information available through a robust, searchable catalog which allows users to find cyber training programs based on location, preferred delivery method, specialty area, or proficiency level. NICCS supports DHS's objective to grow the cyber workforce by providing information about science, technology, engineering, and math (STEM) and cyber-related degree programs, internship and scholarship opportunities, and cyber competitions and events.(1)

To support the workforce development effort the National Institute of Standards and Technology (NIST) on November 1, 2016 announced the release of CyberSeek, an interactive map that shows cybersecurity job availability by both state and locality.

It is one thing to abstractly discuss what cybersecurity professionals do in their positions. However, review a sample of job descriptions and recruitment announcements provide greater insight in to the job duties and required education and qualifications for some of the high paying cybersecurity positions. The job descriptions and recruitment announcements in the last section of this paper were collected in January 2017.

The National Cybersecurity Workforce Framework

The number of cybersecurity-related jobs already outpaces the number of people qualified to fill them, and that demand is growing rapidly. The Department of Homeland Security (DHS) is working with our nation's private industry, academia, and government to develop and maintain an unrivaled, globally competitive cyber workforce.

One of the biggest challenges is the lack of consistency in the way cybersecurity is defined. Job descriptions and titles for the same job roles vary from employer to employer. This makes it harder for universities and colleges to prepare students for their first job. Employers spend time and resources retraining new hires and employees do not have clear career options.

The National Cybersecurity Workforce Framework is the foundation for increasing the size and capability of the U.S. cybersecurity workforce. It provides a common definition of cybersecurity, a comprehensive list of cybersecurity tasks, and the knowledge, skills, and abilities required to perform those tasks. By using the Framework:

- Educators can create programs that are aligned to jobs.
- Students can graduate with knowledge and skills that employers need.
- Employers can recruit from a larger pool of more qualified candidates.
- Employees will have portable skills and better defined career paths and opportunities.
- Policy makers can set standards to promote workforce professionalization.

DHS partnered with industry, academia, and government to develop the Workforce Framework. It is being implement across the Federal Government and is accepted as a best practice resource to define the field of cybersecurity. DHS has also published resources to help employers, educators, and training providers implement the Workforce Framework within their organizations and communities.(2)

The National Cybersecurity Workforce Framework provides a blueprint to categorize, organize, and describe cybersecurity work into Specialty Areas, tasks, and knowledge, skills, and abilities (KSAs). The Workforce Framework provides a common language to speak about cyber roles and jobs and helps define personal requirements in cybersecurity.

Within the Framework, there are seven Categories, each comprising of several Specialty Areas. This organizing structure is based on extensive job analyses that groups together work and workers that share common major functions, regardless of job titles or other occupational terms.

Category One) Analysis specialty areas are responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence:

- All Source Intelligence analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesizes and places intelligence information in context; draws insights about the possible implications.
- Exploitation Analysis specialists analyze collected information to identify vulnerabilities and potential for exploitation.
- Targets specialists apply current knowledge of one or more regions, countries, non-state entities, and/or technologies.

- Threat Analysis specialists identify and assesses the capabilities and activities of cyber criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.

Category Two) Collect and Operate areas are responsible for specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence:

- Collection Operations specialists execute collection using appropriate strategies and within the priorities established through the collection management process.
- Cyber Operations specialists perform activities to gather evidence on criminal or foreign intelligence entities in order to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.
- Cyber Operations Planning specialists perform in-depth joint targeting and cyber planning process. Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conduct strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.

Category Three) Investigate has specialty areas responsible for the investigation of cyber events and/or crimes of IT systems, networks, and digital evidence:

- Digital Forensics specialists collect, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation, and/or criminal, fraud, counterintelligence or law enforcement investigations.

- Investigation specialties apply tactics, techniques, and procedures for a full range of investigative tools and processes to include but not limited to interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.

Category Four) Operate and Maintain has specialty areas responsible for providing the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security:

- Customer Support specialists address problems, installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries.
- Data Administration specialists develop and administers databases and/or data management systems that allow for the storage, query, and utilization of data.
- Knowledge Management specialists manage and administer processes and tools that enable the organization to identify, document, and access intellectual capital and information content.
- Network Services specialists install, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.
- System Administration specialists install, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and

availability. Also manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.

- Systems Security Analysts conduct the integration/testing, operations, and maintenance of systems security.

Category Five) Oversight and Development specialty areas provide leadership, management, direction, and/or development and advocacy so that all individuals and the organization may effectively conduct cybersecurity work:

- Education and Training specialists conduct training of personnel within pertinent subject domain. Develop, plan, coordinate, deliver and/or evaluate training courses, methods, and techniques as appropriate.
- Information Systems Security Operations (Information Systems Security Officer) oversee the information assurance program of an information system in or outside the network environment; may include procurement duties (e.g., ISSO).
- Legal Advice and Advocacy specialists provide legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes, and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.
- Security Program Management (Chief Information Security Officer) manages information security (e.g., information security) implications within the organization, specific program, or other area of responsibility, to include strategic, personnel,

infrastructure, policy enforcement, emergency planning, security awareness, and other resources (e.g., CISO).

- Strategic Planning and Policy Development specialists apply knowledge of priorities to define an entity.

Category Six) Protect and Defend specialty areas are responsible for the identification, analysis, and mitigation of threats to internal IT systems or networks:

- Computer Network Defense Analysts use defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.
- Computer Network Defense Infrastructure Support specialists test, implements, deploys, maintains, reviews and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.
- Incident Response specialists respond to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats and use mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.
- Vulnerability Assessment and Management specialists conduct assessments of threats and vulnerabilities, determine deviations from acceptable configurations, enterprise or

local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.

Category Seven) Securely Provision specialty areas are concerned with conceptualizing, designing, and building secure IT systems, with responsibility for some aspect of the systems' development:

- Information Assurance Compliance specialists oversee, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new IT systems meet the organization's information assurance and security requirements and ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.
- Software Assurance and Security Engineering specialists develop and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.
- Systems Development specialists work on the development phases of the systems development lifecycle.
- Systems Requirements Planning specialists consult with customers to gather and evaluate functional requirements and translate those requirements into technical solutions while providing guidance to customers about applicability of information systems to meet business needs.
- Systems Security Architecture specialists develop system concepts and works on the capabilities phases of the systems development lifecycle; translates technology and

environmental conditions (e.g., law and regulation) into system and security designs and processes.

- Technology Research and Development specialists conduct technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.
- Test and Evaluation specialists develop and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating IT.[3]

Finding Where Jobs are Located

The National Institute of Standards and Technology (NIST) on November 1, 2016 announced the release of CyberSeek, an interactive map that shows cybersecurity job availability by both state and locality (http://cyberseek.org). This interactive tool will assist students, employees, employers, policy makers, training providers and guidance counselors in exploring opportunities they may have never considered. The map uses data collected by the analytics firm Burning Glass Technologies and from the Bureau of Labor Statistics to determine job availability and job fulfillment in certain areas, which then gets displayed like a heat map.

At the time of publication, the map showed nearly 349,000 cybersecurity job openings nationwide and a total employed cybersecurity workforce of more than 778,000.

The CyberSeek website also includes a Career Pathway section, which provides job seekers and those looking to get into cybersecurity careers with entry-level positions, salary statistics, and potential career pathways. The tool is also designed to help employers find areas of the country with a high saturation of cybersecurity workers, as the current market has more open positions than workers able to fill them.

CyberSeek was created by CompTIA and Burning Glass Technologies as the first-year product of a three-year grant awarded to CompTIA by NIST. The first-year grant consisted of $249,000 and CompTIA will receive second-year funding of $110,000 to expand the tool.(4)

Also at CyberSeek there a Cybersecurity Career Pathway tool that shows many opportunities for workers to start and advance their careers within cybersecurity. This interactive career pathway shows key jobs within cybersecurity, common transition opportunities between them, and detailed information about the salaries, credentials, and skill sets associated with each role as well as prevailing salaries.[5]

College Education for Cyber Operations Careers

The National Security Agency's (NSA) National Centers of Academic Excellence (CAE) in Cyber Operations Program supports the President's National Initiative for Cybersecurity Education (NICE): Building a Digital Nation and furthers the goal to broaden the pool of skilled workers capable of supporting a cyber-secure nation.

The CAE-Cyber Operations program is intended to be a deeply technical, inter-disciplinary, higher education program firmly grounded in the computer science (CS), computer engineering (CE), and/or electrical engineering (EE) disciplines, with extensive opportunities for hands-on applications via labs/exercises.

The CAE-Cyber Operations program complements the existing Centers of Academic Excellence (CAE) in Cyber Defense (CAE-CD) programs, providing a particular emphasis on technologies and techniques related to specialized cyber operations (e.g., collection, exploitation, and response), to enhance the national security posture of our Nation. These technologies and techniques are critical to intelligence, military and law enforcement organizations authorized to perform these specialized operations. Below is a list of the current Centers of Academic Excellence in Cyber Operations, the academic years for the designation, and the level of study that has met the criteria:

- Air Force Institute of Technology (Ohio) 2013-2018 (Graduate) M.S. in Cyber Operations