Free Cybersecurity Training:

U.S. Government Sources

Edited by

Michael Erbschloe

Connect with Michael on LinkedIn

Table of Contents

Section	Page Number
About the Editor	3
Introduction	4
National Cybersecurity Workforce Framework.	7
Free Cybersecurity Training	15
Finding Where Jobs are Located	59
Cybersecurity Acronyms	61

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

America has about 5.5 million open jobs today. Over half a million job openings are in information technology fields such as software development, network administration, and cybersecurity — rapidly growing sectors with many more jobs than just a decade ago. Whether in manufacturing, advertising, retail or banking, the average salary in a job that requires information technology (IT) skills is 50 percent higher than the average private-sector American job.

As of 2016 Businesses have added 13.5 million jobs over 68 straight months of private-sector job growth, extending the longest streak on record. While this progress is significant, employers are in critical need of tech talent and too many Americans lack the skills and experience to access these well-paying jobs. Over six million young Americans between the ages of 16 and 24 are out of school and work, which represents a significant untapped resource of productivity and talent for the country.

Today's world is more interconnected than ever before. Yet, for all its advantages, increased connectivity brings increased risk of theft, fraud, and abuse. As Americans become more reliant on modern technology, we also become more vulnerable to cyber attacks such as corporate security breaches, spear phishing, and social media fraud. Complementary cybersecurity and law enforcement capabilities are critical to safeguarding and securing cyberspace. Law enforcement performs an essential role in achieving our nation's cybersecurity objectives by investigating a wide range of cyber crimes, from theft and fraud to child exploitation, and apprehending and prosecuting those responsible. The Department of Homeland Security (DHS) works with other federal agencies to conduct high-impact criminal investigations to disrupt and defeat cyber criminals, prioritize the recruitment and training of technical experts, develop standardized methods, and broadly share cyber response best practices and tools. Criminal investigators and network security experts with deep understanding of the technologies malicious actors are using and the specific vulnerabilities they are targeting work to effectively respond to and investigate cyber incidents.

(Link: https://www.dhs.gov/topic/combating-cyber-crime)

Consider this:

- Within the past year, personally identifiable information has been stolen in a number of significant cyber data breaches, impacting industries like health care, government, finance, corporate, and retail.
- The use of malware by online criminals continues unabated, and of the available intrusion devices, the "bot" is particularly pervasive, allowing attackers to take control remotely of compromised computers. Once in place, these "botnets" can be used in distributed denial-of-service attacks, proxy and spam services, additional malware distribution, and other organized criminal activity.
- Cyber criminals perpetrate a wide variety of crimes online, including theft of intellectual property, Internet fraud, identity fraud, and any number of financial fraud schemes.
- Sexual predators use the Internet and social media to target the youngest and most vulnerable victims.
- And many criminals use the so-called "dark web" or "dark market" websites that offer a range of illegal goods and services for sale on a network designed to conceal the true IP addresses of the computers on it.

The FBI—working in conjunction with its many partners at the local, state, federal, and international levels, as well as with industry—takes its own role in cyber security very seriously. That role involves operational efforts—including investigating and disrupting cyber-related national security threats and cyber crimes and collecting, analyzing, and disseminating cyber threat intelligence. It also involves outreach efforts to industry. Here are just a few examples of how we're doing all of that:

- The FBI-led National Cyber Joint Investigative Task Force serves as the national focal point for coordinating cyber threat investigations. The work of the NCJITF includes a national public/private initiative to mitigate the use of botnets and malware by criminals, which has emerged as a global cyber security threat.
- Cyber task forces in all 56 field offices coordinate domestic cyber threat investigations in local communities through information sharing, incident response, and joint enforcement and intelligence actions.
- InfraGard—an information-sharing and analysis effort with private sector partners who own, operate, and hold key positions within some 85 percent of the nation's critical infrastructure—equips its members to identify and mitigate vulnerabilities, develop incident response plans, and enact security best practices.

- The Internet Crime Complaint Center (IC3) accepts online submissions for Internet-related crime complaints, often involving fraudulent claims to consumers. These complaints can not only lead to culprits getting caught, but also help identify regional, national, or international trends to educate the public about constantly evolving cyber threats and scams.
- The FBI's Safe Online Surfing website, an online program that promotes cyber citizenship by educating young students in the essentials of online security in an effort to help protect them from child predators, cyber bullies, malware, a multitude of schemes, and other dangers on the Internet.

(Link: https://www.fbi.gov/news/stories/national-cyber-security-awareness-month)

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.

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.

Link: http://csrc.nist.gov/nice/framework/

Free Cybersecurity Training

Federal Virtual Training Environment (FedVTE)

Federal Virtual Training Environment (FedVTE) is a free online, on-demand cybersecurity training system that is available at **no charge to for government personnel and veterans**. Managed by DHS, FedVTE contains more than 800 hours of training on topics such as ethical hacking and surveillance, risk management, and malware analysis. Course proficiency ranges from beginner to advanced levels. Several courses align with a variety of IT certifications such as Network +, Security +, and Certified Information Systems Security Professional (CISSP).

Veterans who have served and protected the Nation are well-positioned to transition into much needed jobs. To celebrate National Military Appreciation Month, DHS released the Veterans Cybersecurity Training and Education Guide to help veterans enter this career field. Did you know that cybersecurity professionals report an average salary of $116,000? That’s nearly three times the national average. The demand for cybersecurity experts is growing 12 times faster than the current U.S. job market, making cybersecurity one of the most highly sought-after careers in the country.

Veteran Registration: Registration: Go to fedvte.usalearning.gov to register

Links

https://niccs.us-cert.gov/training/federal-virtual-training-environment-fedvte

https://niccs.us-cert.gov/training/veterans

Cybersecurity for Small Businesses from the SBA Learning Center

This self-paced training exercise provides an introduction to securing information in a small business. Topics include: Defining cybersecurity; Explaining the importance of securing information through best cybersecurity practices; Identifying types of information that should be secured; Identifying the types of cyber threats; Defining risk management; and Listing best practices for guarding against cyber threats. Duration: 00:30:00

Links

Online version: https://www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses

Text version: https://www.sba.gov/sites/default/files/cybersecurity_transcript_0.pdf

Other courses are available from the same source:

https://business.usa.gov/training-materials/online%20training/