Module 1
Security Fundamentals

Submodule 3: Cybersecurity Profession & Careers

Submodule Learning Outcomes:

Explain what cybersecurity entails as a profession

Enumerate typical cybersecurity working roles

Demonstrate knowledge about resources for cybersecurity education and training

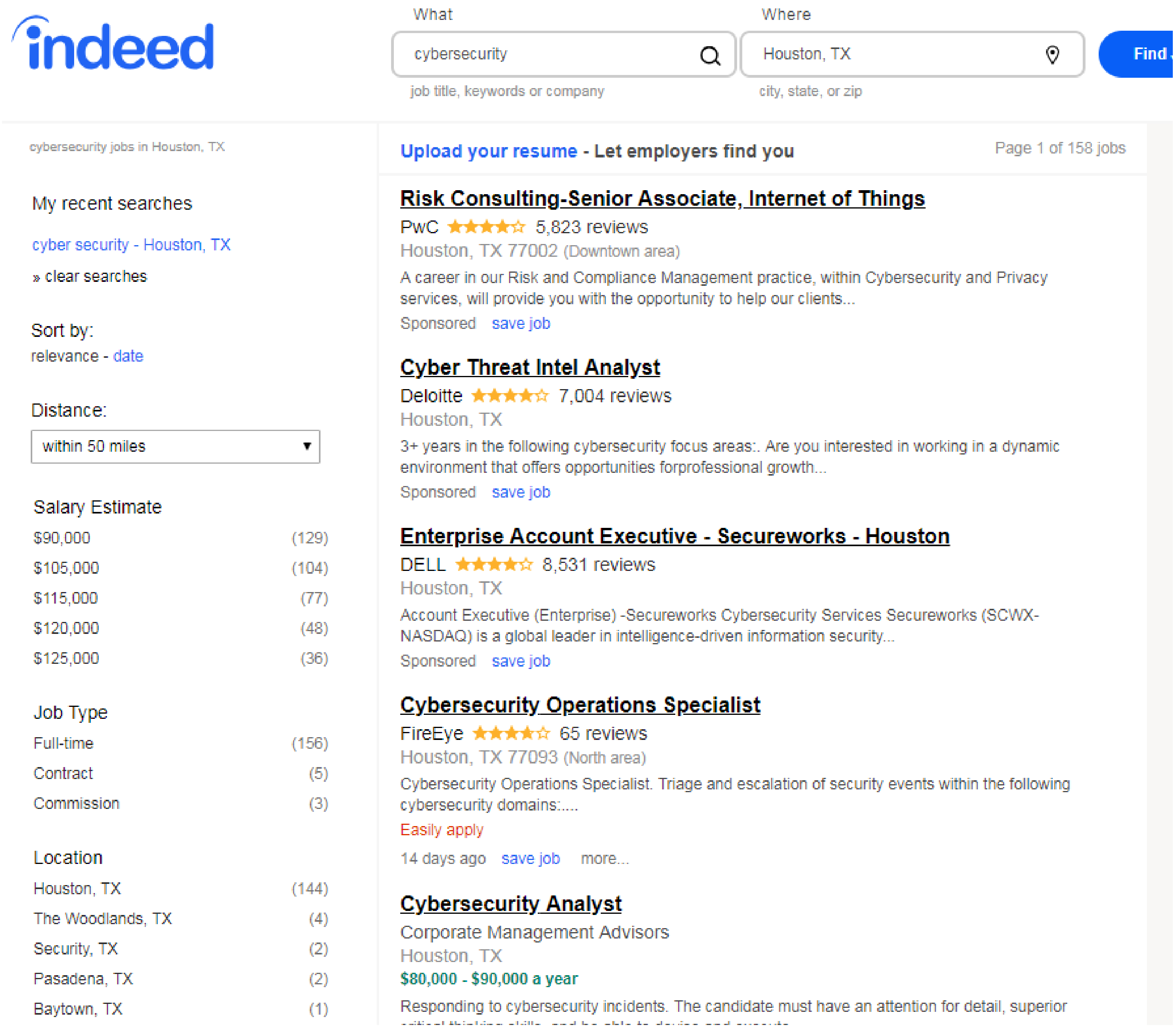
What is Cybersecurity?

- Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. (from cisco.com)

- Cybersecurity professional are those who can provide various types of such protection.

Who Are Hiring?

- Government agencies
- Defense contractors
- Private sectors
  - Healthcare
  - Finance
  - Manufacturing
  - Retail
  - …



What: cybersecurity
job title, keywords or company

Where: Houston, TX
city, state, or zip

cybersecurity jobs in Houston, TX

Upload your resume - Let employers find you

Page 1 of 158 jobs

My recent searches

cyber security - Houston, TX

» clear searches

Sort by:
relevance - date

Distance:
within 50 miles ▾

Salary Estimate

$90,000	(129)
$105,000	(104)
$115,000	(77)
$120,000	(48)
$125,000	(36)

Job Type

Full-time	(156)
Contract	(5)
Commission	(3)

Location

Houston, TX	(144)
The Woodlands, TX	(4)
Security, TX	(2)
Pasadena, TX	(2)
Baytown, TX	(1)

Risk Consulting-Senior Associate, Internet of Things
PwC ★★★★☆ 5,823 reviews
Houston, TX 77002 (Downtown area)
A career in our Risk and Compliance Management practice, within Cybersecurity and Privacy services, will provide you with the opportunity to help our clients...
Sponsored save job

Cyber Threat Intel Analyst
Deloitte ★★★★☆ 7,004 reviews
Houston, TX
3+ years in the following cybersecurity focus areas:. Are you interested in working in a dynamic environment that offers opportunities forprofessional growth...
Sponsored save job

Enterprise Account Executive - Secureworks - Houston
DELL ★★★★☆ 8,531 reviews
Houston, TX
Account Executive (Enterprise) -Secureworks Cybersecurity Services Secureworks (SCWX-NASDAQ) is a global leader in intelligence-driven information security...
Sponsored save job

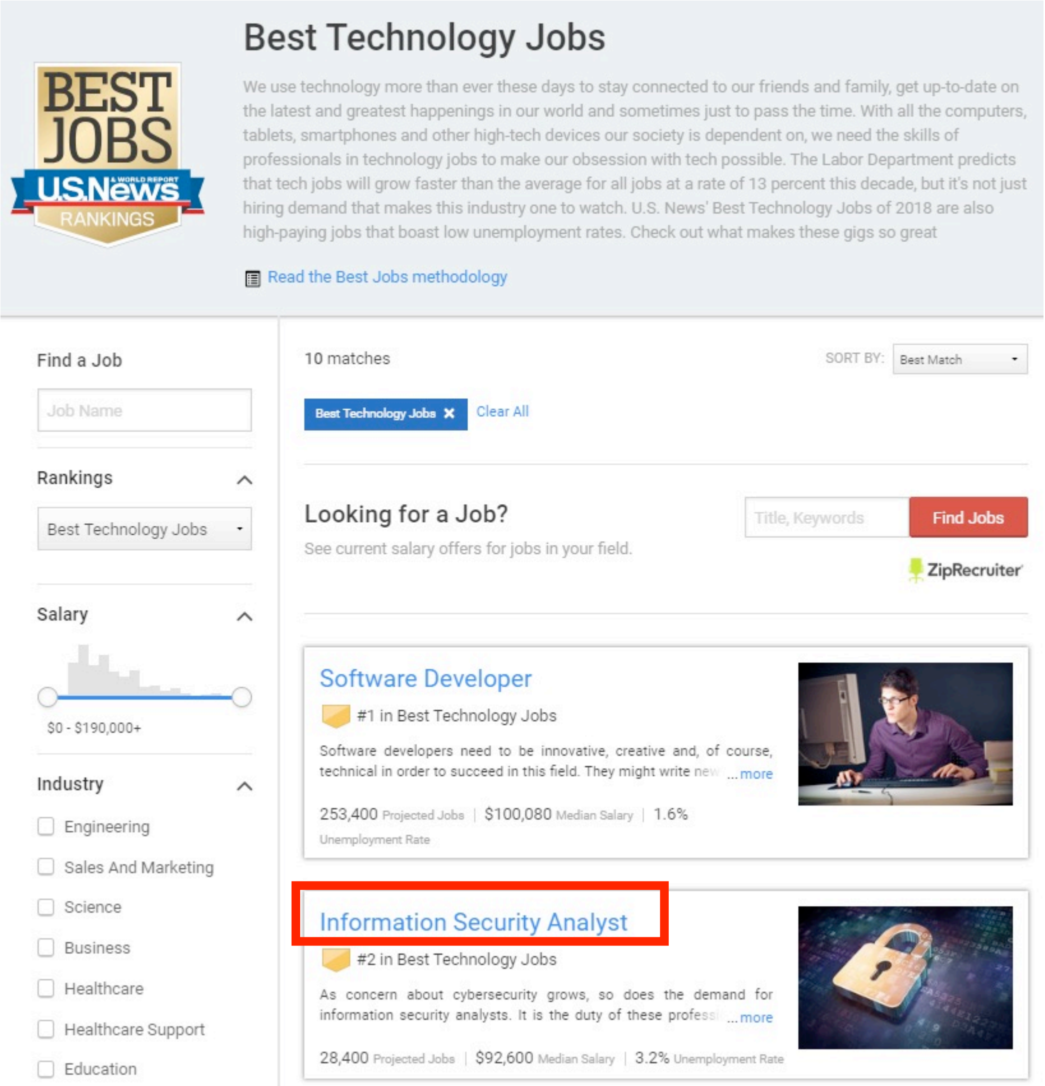
Cybersecurity Operations Specialist
FireEye ★★★★☆ 65 reviews
Houston, TX 77093 (North area)
Cybersecurity Operations Specialist. Triage and escalation of security events within the following cybersecurity domains:....
Easily apply
14 days ago save job more...

Cybersecurity Analyst
Corporate Management Advisors
Houston, TX
$80,000 - $90,000 a year
Responding to cybersecurity incidents. The candidate must have an attention for detail, superior

Cybersecurity Workforce Shortage

- The Global Information Security Workforce Study finds that the cybersecurity workforce gap is on pace to hit 1.8 million by 2022 – a 20% increase since 2015.
- According to CSO.com, it is estimated that there are 350,000 open cybersecurity positions in the US. It is predicted that we will see a global shortfall of 3.5 million cybersecurity jobs by 2021.

Money Talks



Best Technology Jobs

We use technology more than ever these days to stay connected to our friends and family, get up-to-date on the latest and greatest happenings in our world and sometimes just to pass the time. With all the computers, tablets, smartphones and other high-tech devices our society is dependent on, we need the skills of professionals in technology jobs to make our obsession with tech possible. The Labor Department predicts that tech jobs will grow faster than the average for all jobs at a rate of 13 percent this decade, but it's not just hiring demand that makes this industry one to watch. U.S. News' Best Technology Jobs of 2018 are also high-paying jobs that boast low unemployment rates. Check out what makes these gigs so great

Read the Best Jobs methodology

10 matches

Looking for a Job?

See current salary offers for jobs in your field.

Software Developer

#1 in Best Technology Jobs

Software developers need to be innovative, creative and, of course, technical in order to succeed in this field. They might write new ...more

253,400 Projected Jobs | $100,080 Median Salary | 1.6% Unemployment Rate

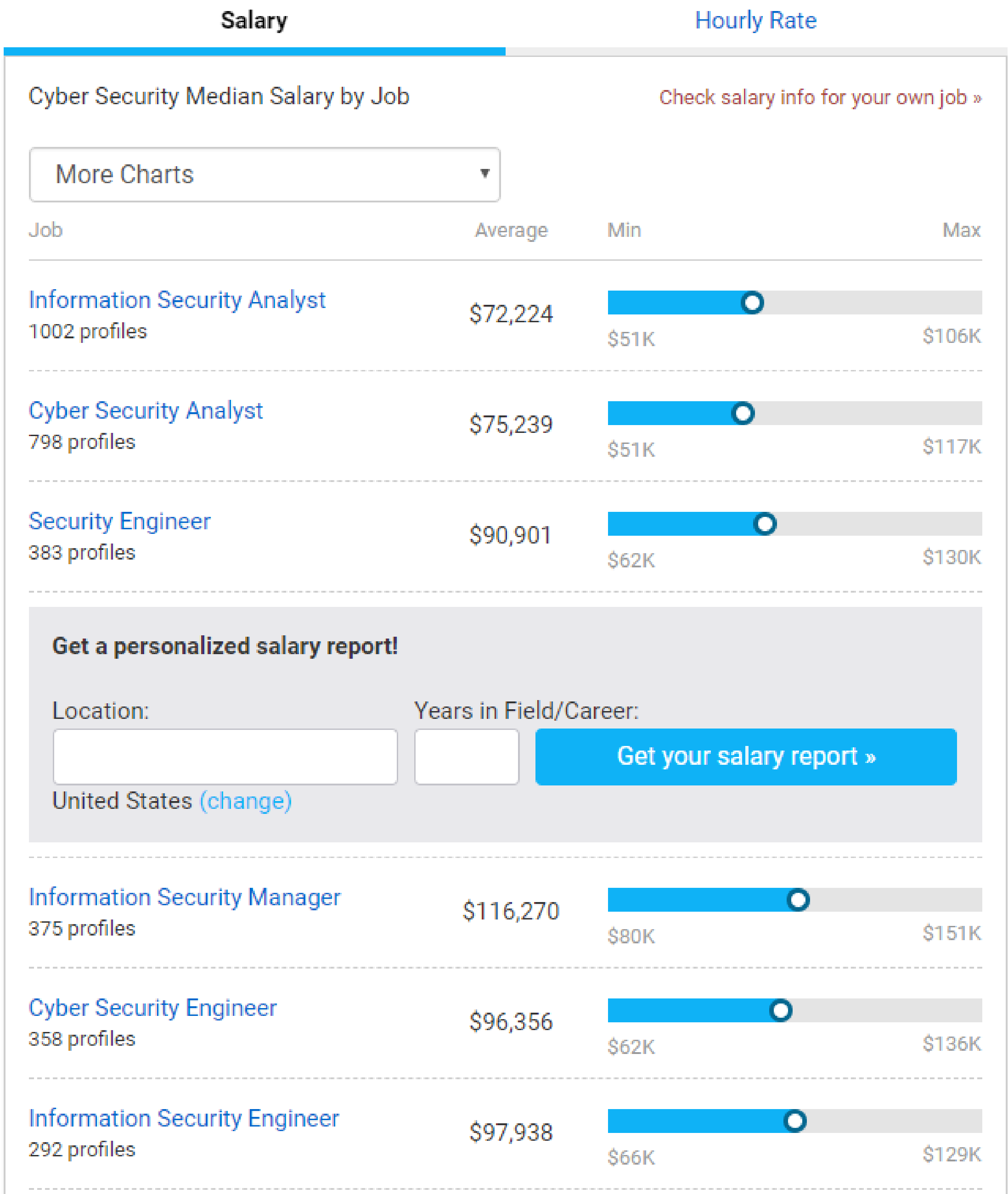
Information Security Analyst

#2 in Best Technology Jobs

As concern about cybersecurity grows, so does the demand for information security analysts. It is the duty of these professi ...more

28,400 Projected Jobs | $92,600 Median Salary | 3.2% Unemployment Rate

The Bureau of Labor Statistics expects “Information Security Analysis” positions to grow at a rate of 18 percent through 2024.



Cyber Security Median Salary by Job

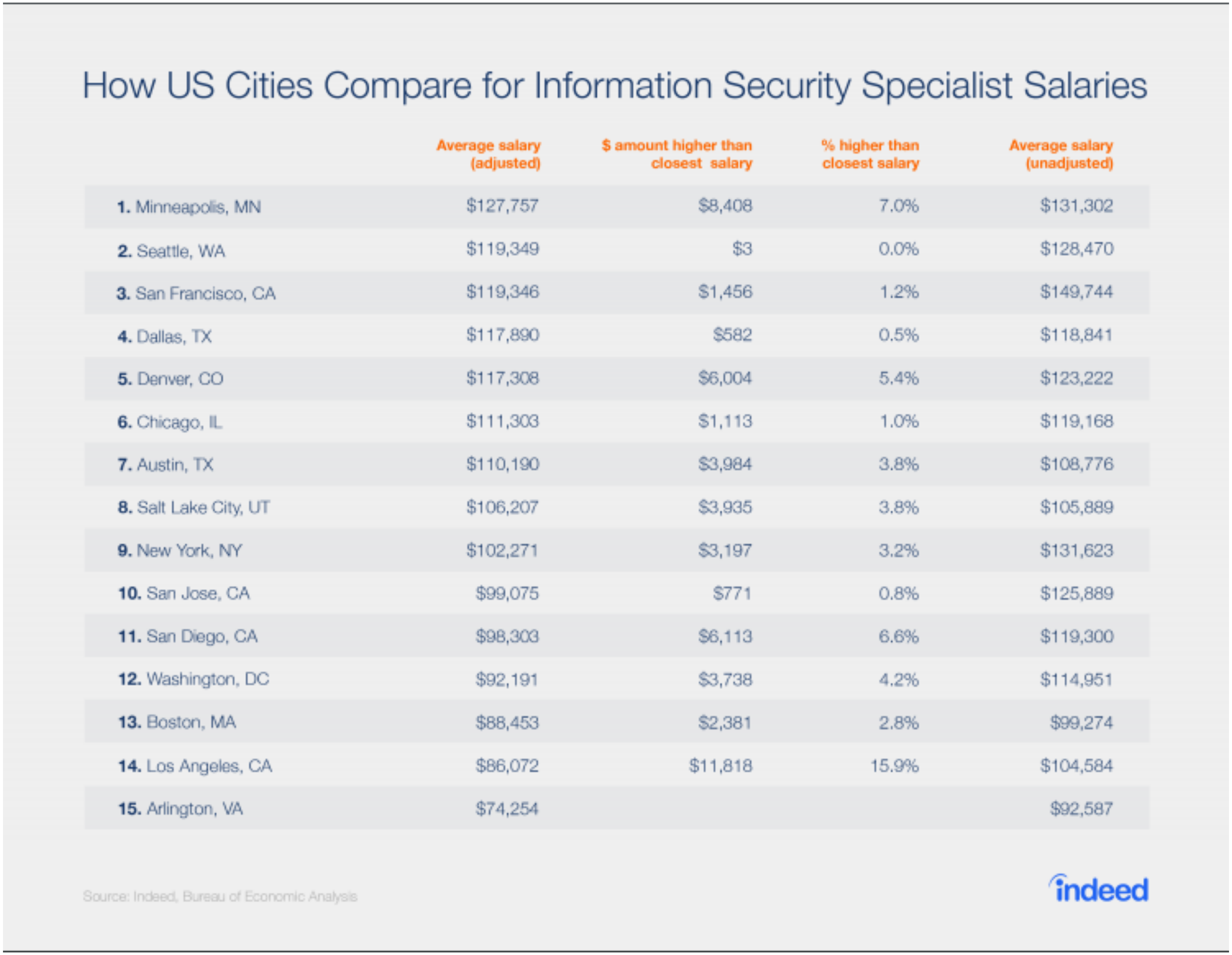
Job	Average	Min	Max
Information Security Analyst 1002 profiles	$72,224	$51K	$106K
Cyber Security Analyst 798 profiles	$75,239	$51K	$117K
Security Engineer 383 profiles	$90,901	$62K	$130K
Information Security Manager 375 profiles	$116,270	$80K	$151K
Cyber Security Engineer 358 profiles	$96,356	$62K	$136K
Information Security Engineer 292 profiles	$97,938	$66K	$129K

Get a personalized salary report!

Location:

Years in Field/Career:

United States (change)



How US Cities Compare for Information Security Specialist Salaries

	Average salary (adjusted)	$ amount higher than closest salary	% higher than closest salary	Average salary (unadjusted)
1. Minneapolis, MN	$127,757	$8,408	7.0%	$131,302
2. Seattle, WA	$119,349	$3	0.0%	$128,470
3. San Francisco, CA	$119,346	$1,456	1.2%	$149,744
4. Dallas, TX	$117,890	$582	0.5%	$118,841
5. Denver, CO	$117,308	$6,004	5.4%	$123,222
6. Chicago, IL	$111,303	$1,113	1.0%	$119,168
7. Austin, TX	$110,190	$3,984	3.8%	$108,776
8. Salt Lake City, UT	$106,207	$3,935	3.8%	$105,889
9. New York, NY	$102,271	$3,197	3.2%	$131,623
10. San Jose, CA	$99,075	$771	0.8%	$125,889
11. San Diego, CA	$98,303	$6,113	6.6%	$119,300
12. Washington, DC	$92,191	$3,738	4.2%	$114,951
13. Boston, MA	$88,453	$2,381	2.8%	$99,274
14. Los Angeles, CA	$86,072	$11,818	15.9%	$104,584
15. Arlington, VA	$74,254			$92,587

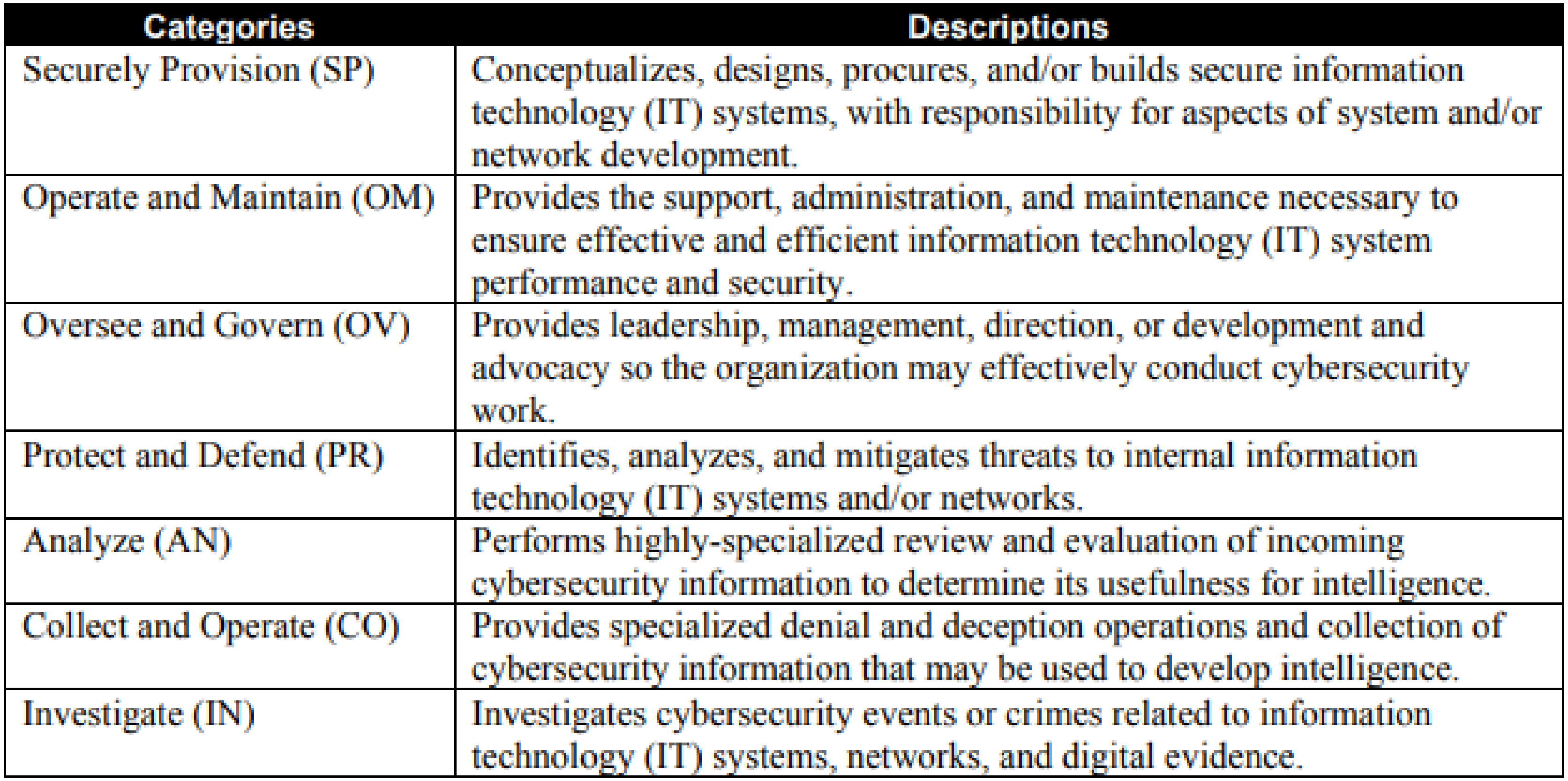
Source: Indeed, Bureau of Economic Analysis

indeed

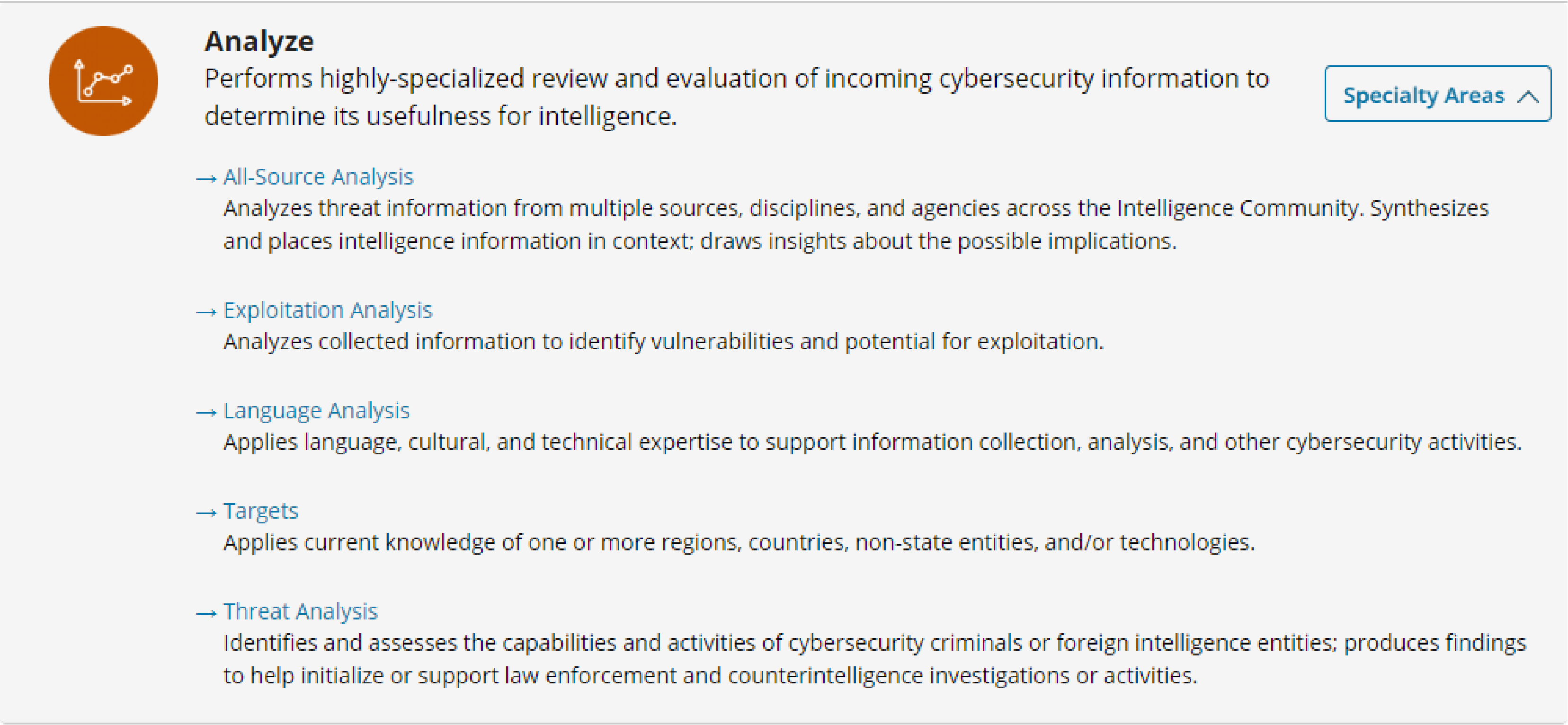
What Jobs Are Out There?

- There is a wide range of jobs in the general cybersecurity field.
- NICE Cybersecurity Workforce Framework (NCWF):
  - Created by the National Initiative for Cybersecurity Education (NICE)
  - Provides a blueprint to categorize, organize, and describe cybersecurity work into Categories, Specialty Areas, Work Roles, tasks, and knowledge, skills, and abilities (KSAs)
  - You can find the full version of the framework here.

NCWF Categories



Categories	Descriptions
Securely Provision (SP)	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.
Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
Analyze (AN)	Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Collect and Operate (CO)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Investigate (IN)	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.



Analyze

Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

→ All-Source Analysis

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

Analyzes collected information to identify vulnerabilities and potential for exploitation.

→ Language Analysis

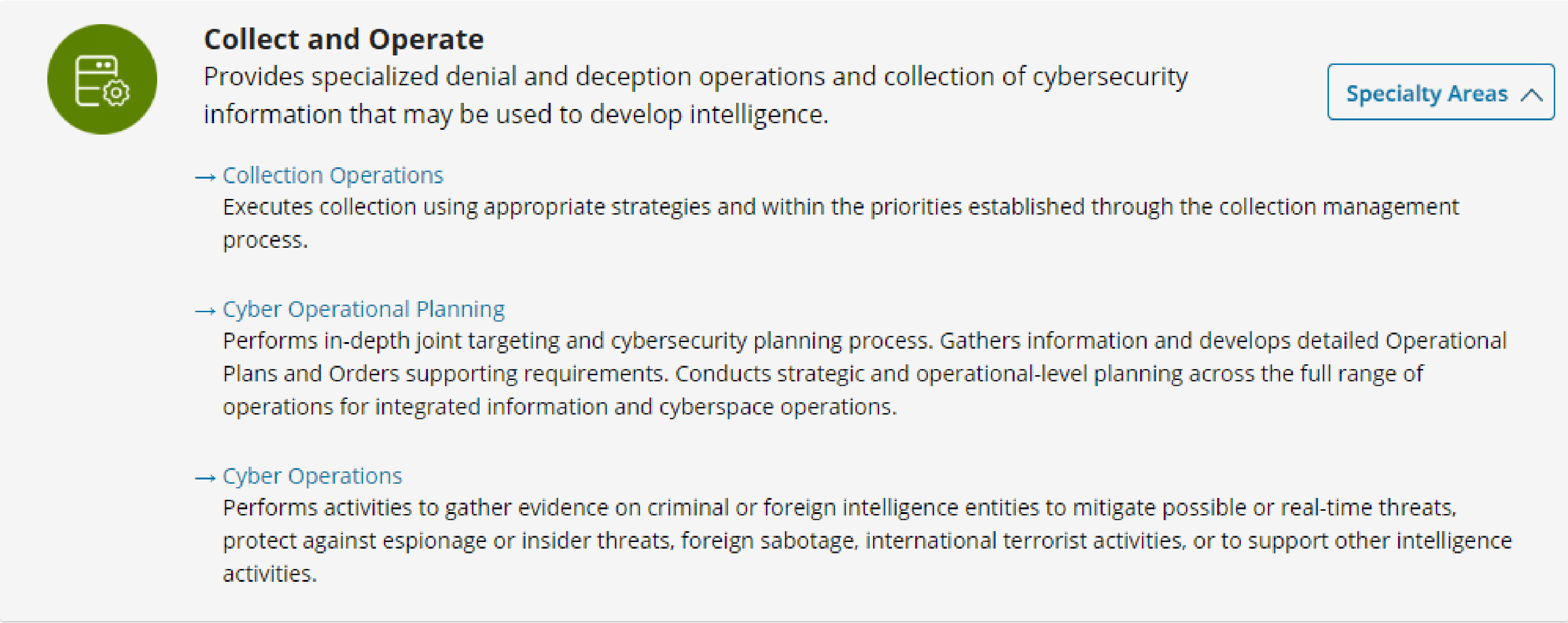
Applies language, cultural, and technical expertise to support information collection, analysis, and other cybersecurity activities.

→ Targets

Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.

→ Threat Analysis

Identifies and assesses the capabilities and activities of cybersecurity criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.



Collect and Operate

Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.

→ Collection Operations

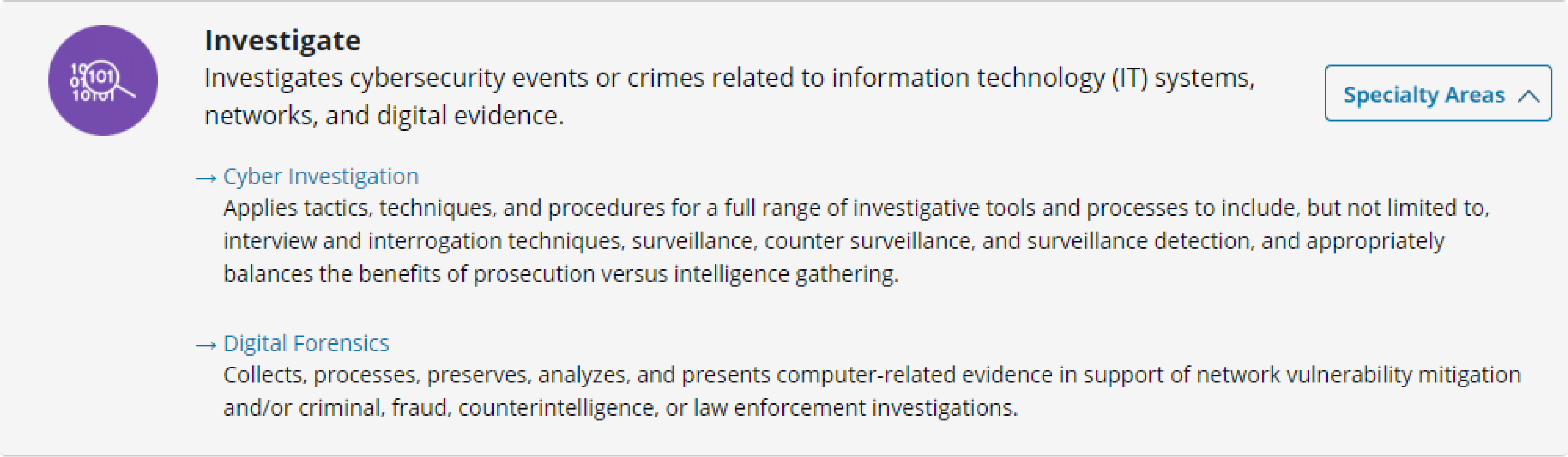
Executes collection using appropriate strategies and within the priorities established through the collection management process.

→ Cyber Operational Planning

Performs in-depth joint targeting and cybersecurity planning process. Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.

→ Cyber Operations

Performs activities to gather evidence on criminal or foreign intelligence entities to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.



Investigate

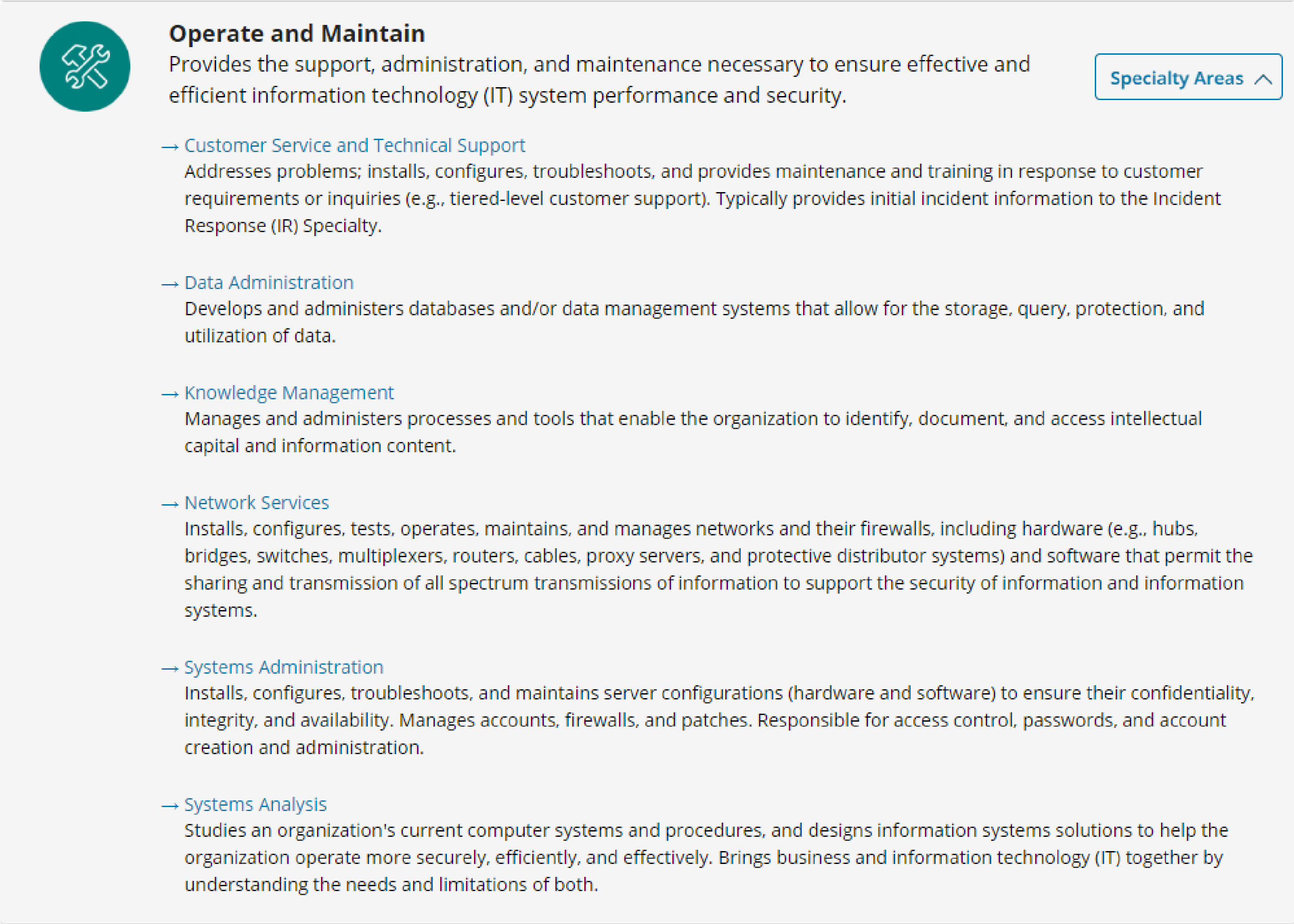
Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

→ Cyber Investigation

Applies 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.

→ Digital Forensics

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



Operate and Maintain

Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.

→ Customer Service and Technical Support

Addresses problems; installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support). Typically provides initial incident information to the Incident Response (IR) Specialty.

→ Data Administration

Develops and administers databases and/or data management systems that allow for the storage, query, protection, and utilization of data.

→ Knowledge Management

Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.

→ Network Services

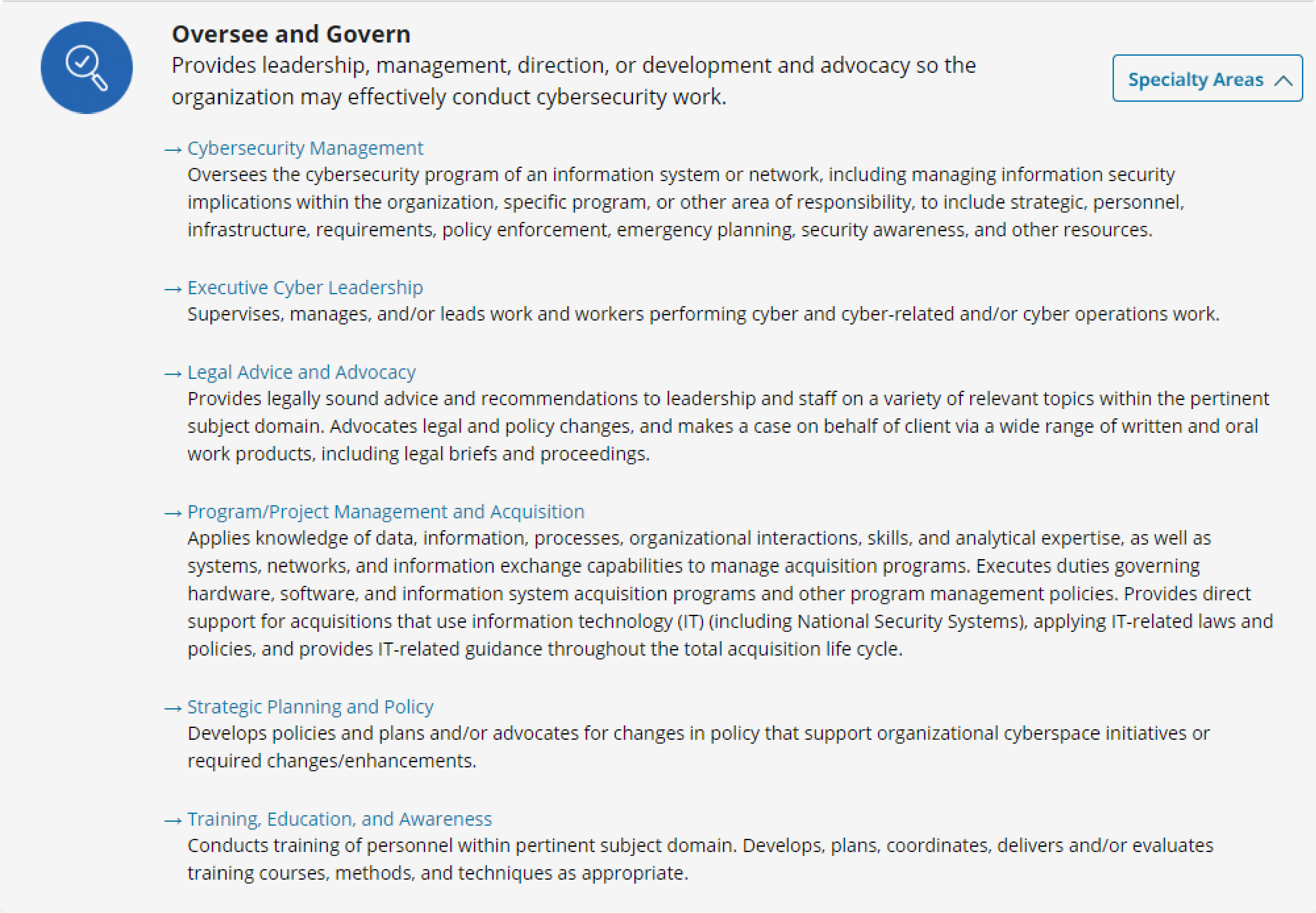
Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.

→ Systems Administration

Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.

→ Systems Analysis

Studies an organization's current computer systems and procedures, and designs information systems solutions to help the organization operate more securely, efficiently, and effectively. Brings business and information technology (IT) together by understanding the needs and limitations of both.



Oversee and Govern

Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.

→ Cybersecurity Management

Oversees the cybersecurity program of an information system or network, including managing information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, requirements, policy enforcement, emergency planning, security awareness, and other resources.

→ Executive Cyber Leadership

Supervises, manages, and/or leads work and workers performing cyber and cyber-related and/or cyber operations work.

→ Legal Advice and Advocacy

Provides 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.

→ Program/Project Management and Acquisition

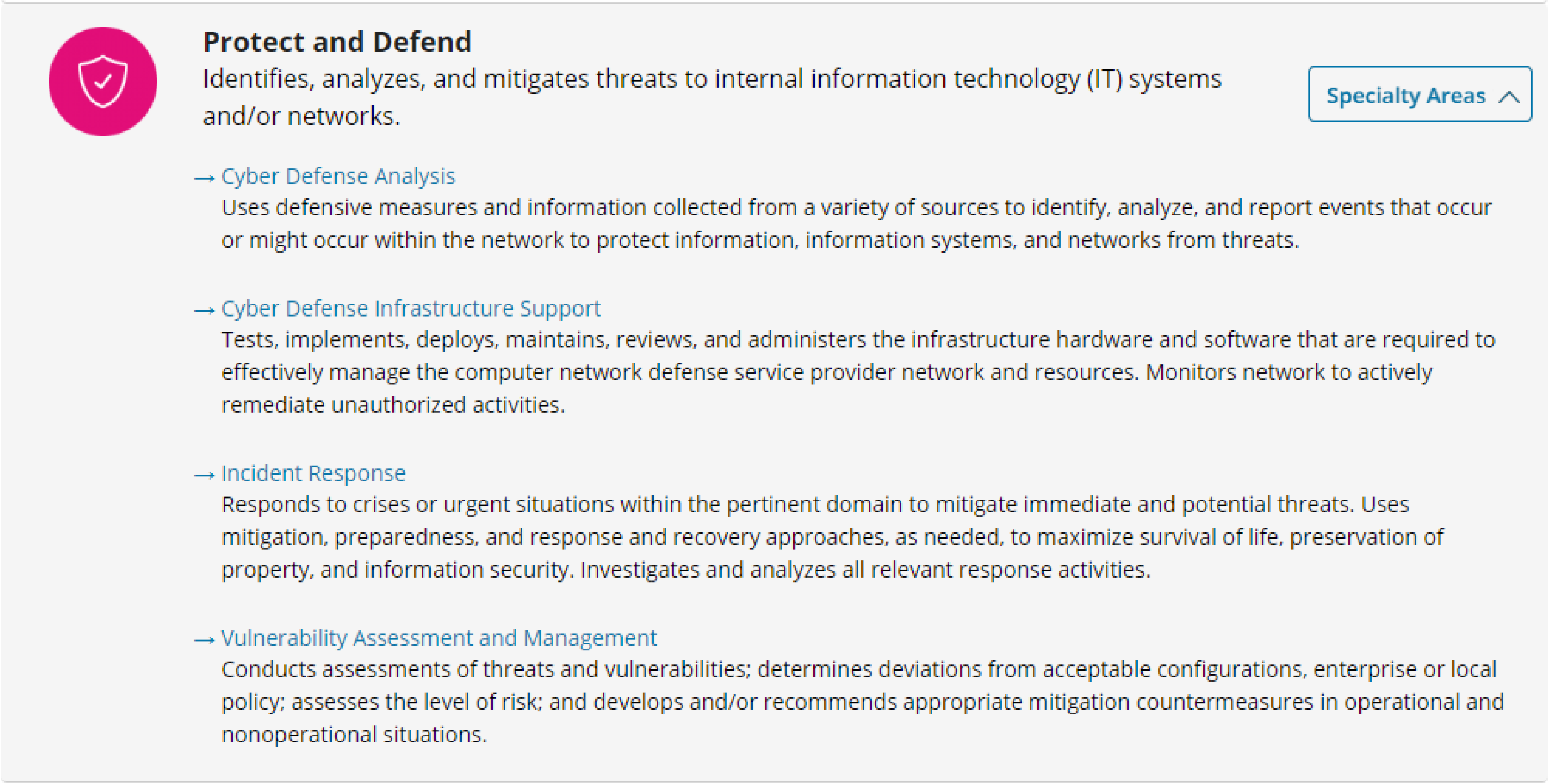
Applies knowledge of data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information exchange capabilities to manage acquisition programs. Executes duties governing hardware, software, and information system acquisition programs and other program management policies. Provides direct support for acquisitions that use information technology (IT) (including National Security Systems), applying IT-related laws and policies, and provides IT-related guidance throughout the total acquisition life cycle.

→ Strategic Planning and Policy

Develops policies and plans and/or advocates for changes in policy that support organizational cyberspace initiatives or required changes/enhancements.

→ Training, Education, and Awareness

Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers and/or evaluates training courses, methods, and techniques as appropriate.



Protect and Defend

Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.

→ Cyber Defense Analysis

Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network to protect information, information systems, and networks from threats.

→ Cyber Defense Infrastructure Support

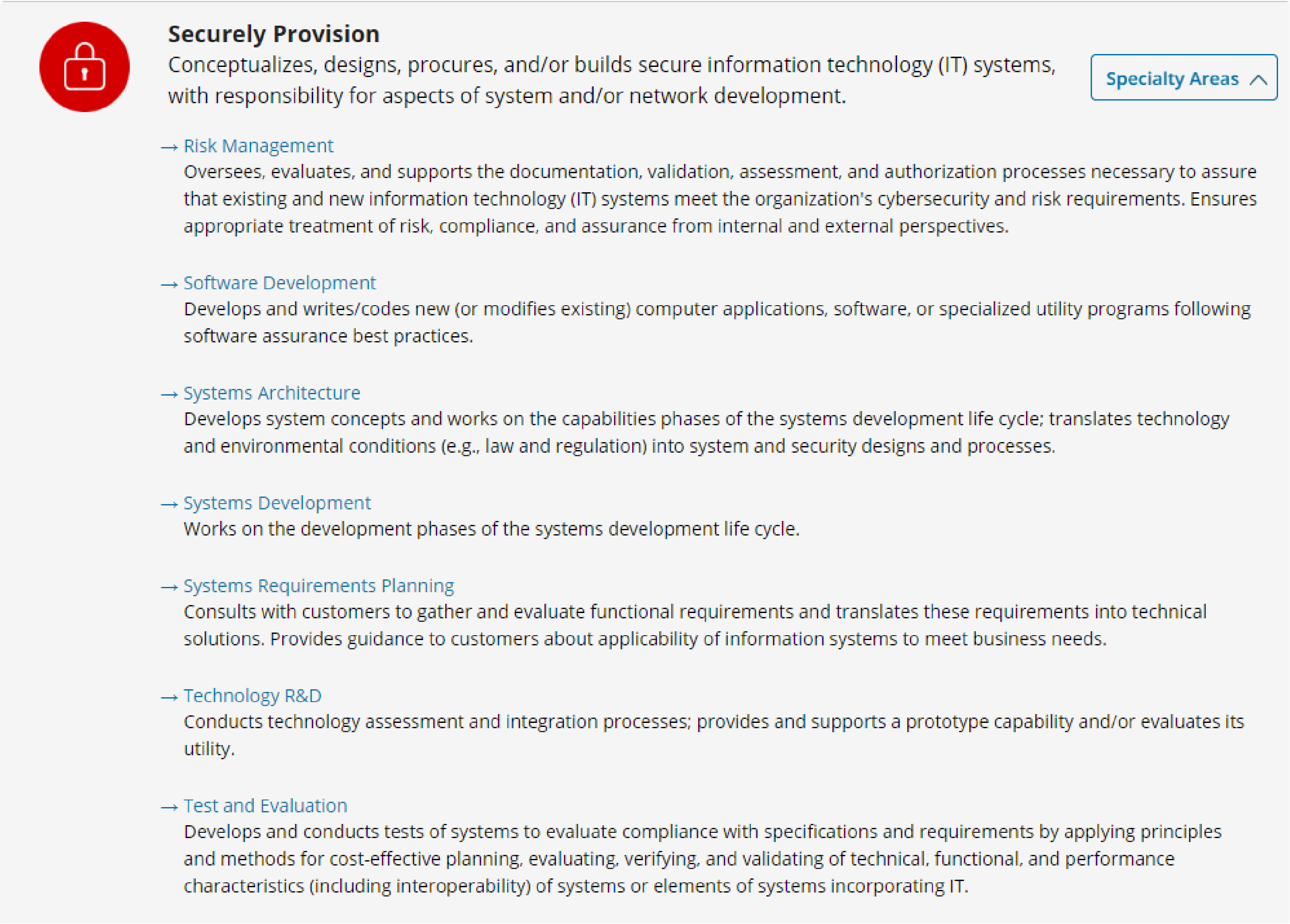
Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.

→ Incident Response

Responds to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses 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

Conducts assessments of threats and vulnerabilities; determines deviations from acceptable configurations, enterprise or local policy; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations.



Securely Provision

Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.

→ Risk Management

Oversees, evaluates, and supports the documentation, validation, assessment, and authorization processes necessary to assure that existing and new information technology (IT) systems meet the organization's cybersecurity and risk requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.

→ Software Development

Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.

→ Systems Architecture

Develops system concepts and works on the capabilities phases of the systems development life cycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.

→ Systems Development

Works on the development phases of the systems development life cycle.

→ Systems Requirements Planning

Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.

→ Technology R&D

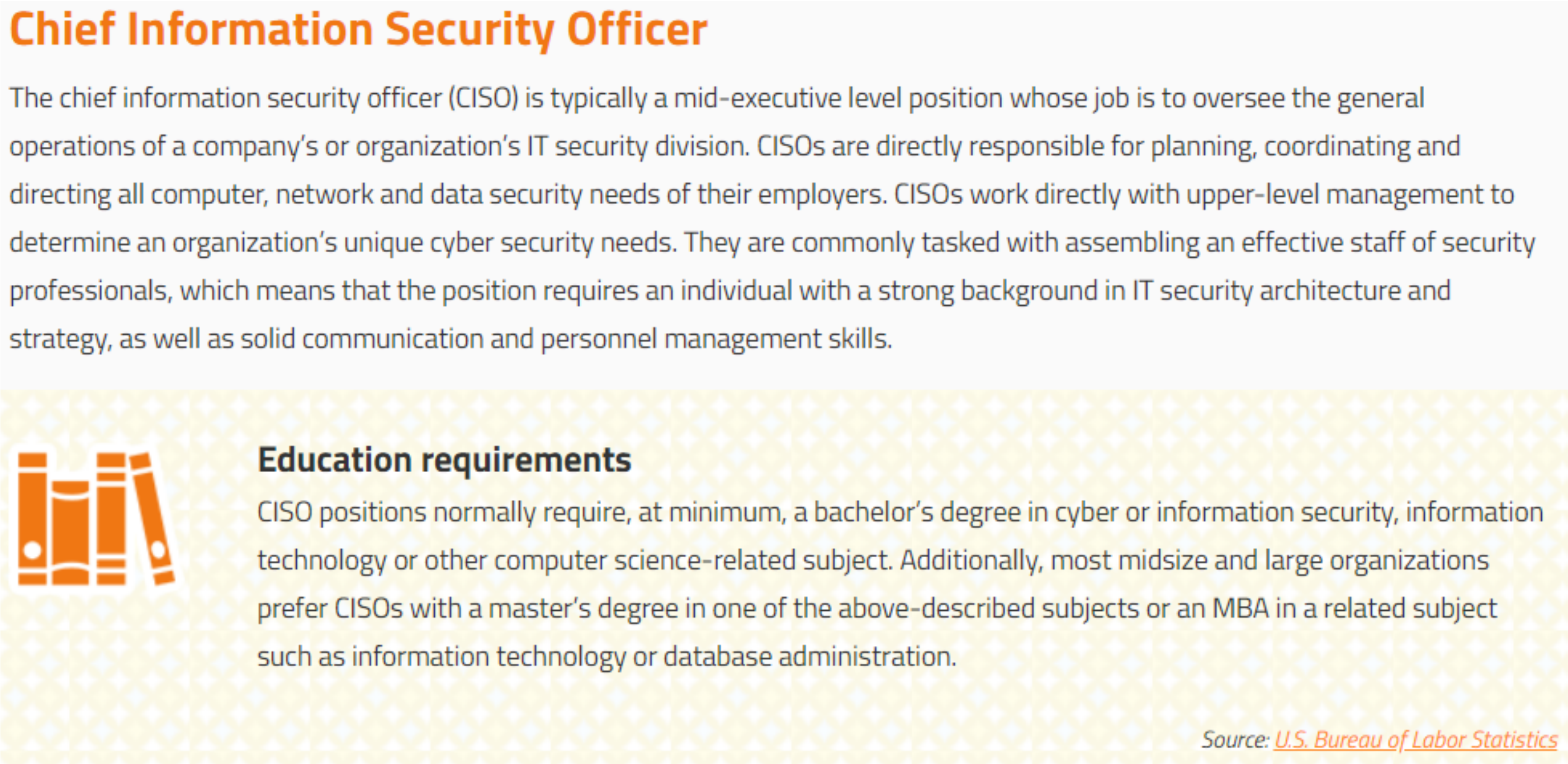
Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.

→ Test and Evaluation

Develops 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.

Career Paths in Cybersecurity

- Some possible career paths are as follows:
    - Chief Information Security Officer
    - Forensic Computer Analyst
    - Information Security Analyst
    - Penetration Tester
    - Security Architect
    - IT Security Engineer
    - Security Systems Administrator
    - IT Security Consultant



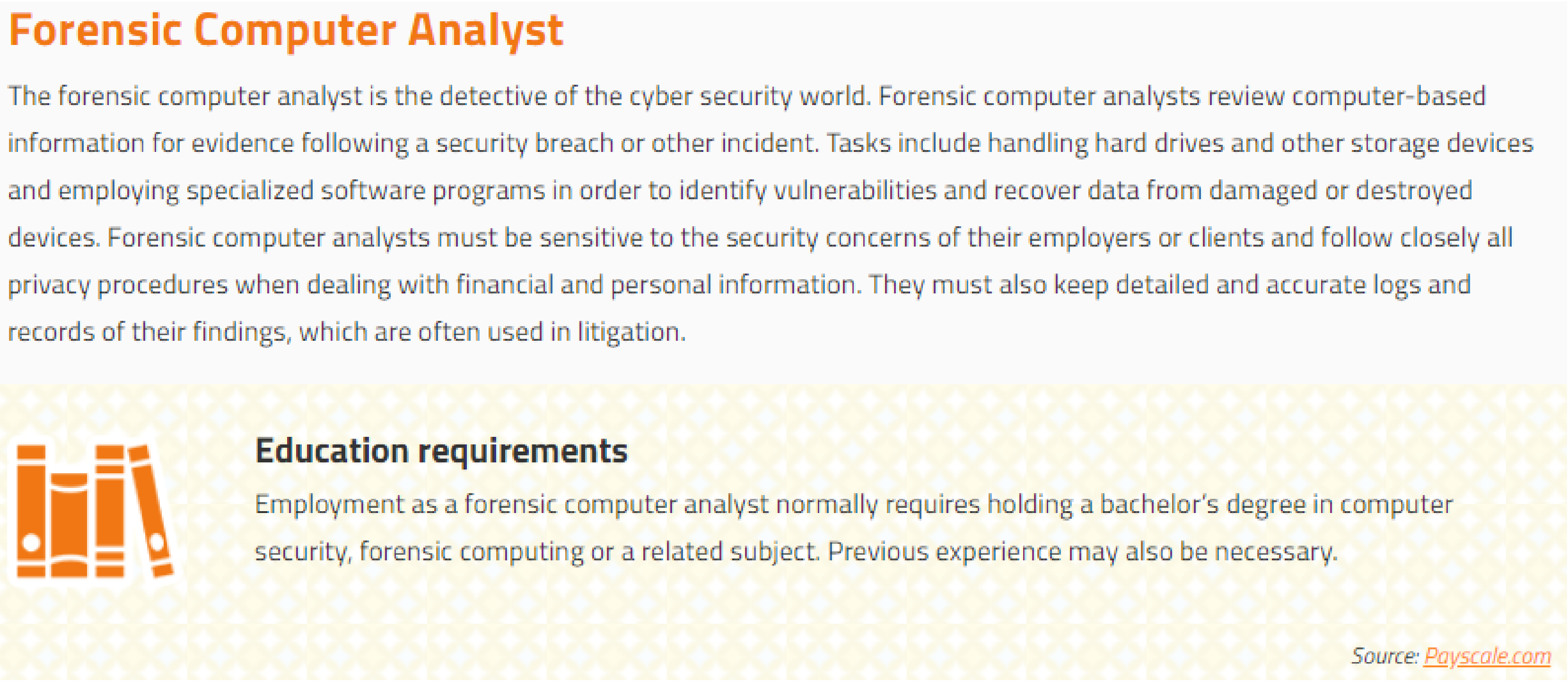
Chief Information Security Officer

The chief information security officer (CISO) is typically a mid-executive level position whose job is to oversee the general operations of a company's or organization's IT security division. CISOs are directly responsible for planning, coordinating and directing all computer, network and data security needs of their employers. CISOs work directly with upper-level management to determine an organization's unique cyber security needs. They are commonly tasked with assembling an effective staff of security professionals, which means that the position requires an individual with a strong background in IT security architecture and strategy, as well as solid communication and personnel management skills.

Education requirements

CISO positions normally require, at minimum, a bachelor's degree in cyber or information security, information technology or other computer science-related subject. Additionally, most midsize and large organizations prefer CISOs with a master's degree in one of the above-described subjects or an MBA in a related subject such as information technology or database administration.

Source: U.S. Bureau of Labor Statistics



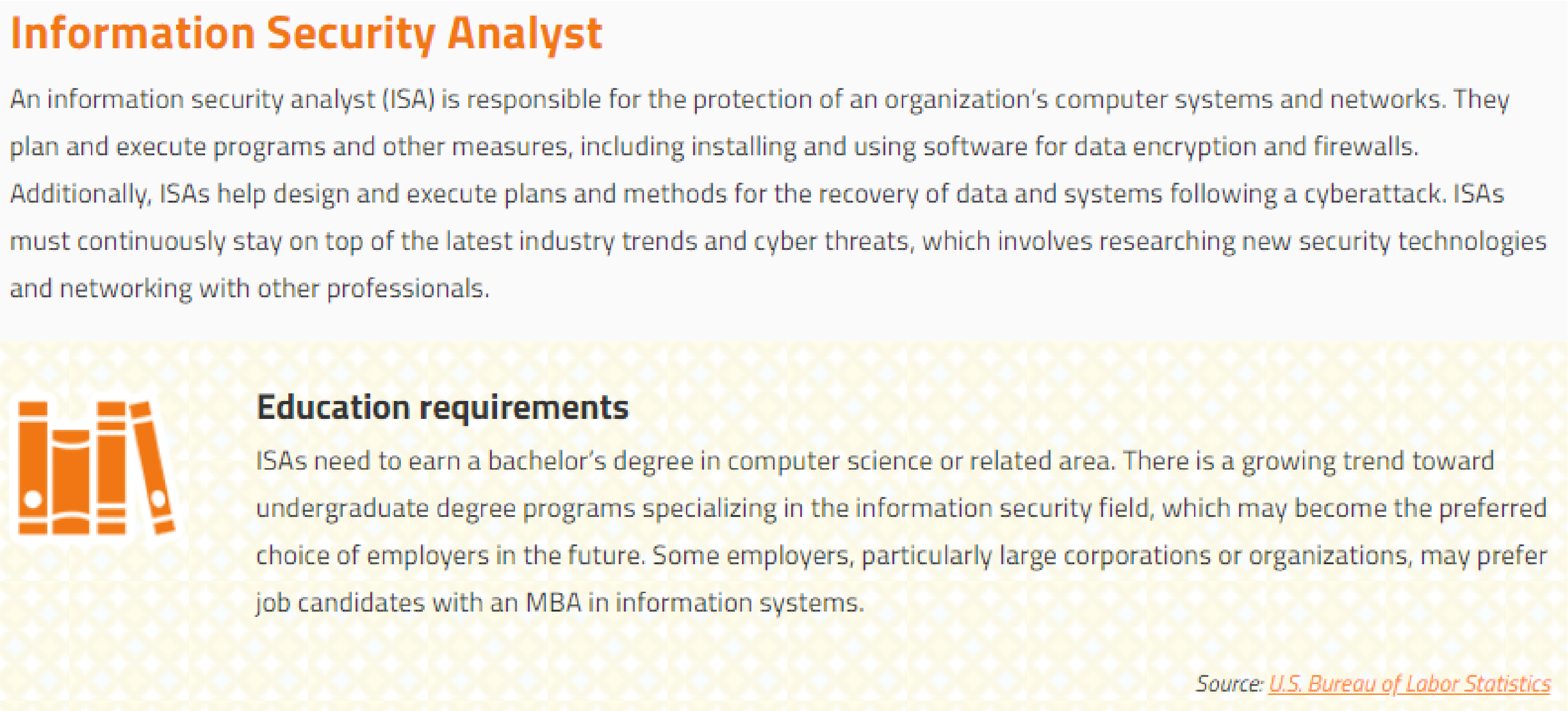
Forensic Computer Analyst

The forensic computer analyst is the detective of the cyber security world. Forensic computer analysts review computer-based information for evidence following a security breach or other incident. Tasks include handling hard drives and other storage devices and employing specialized software programs in order to identify vulnerabilities and recover data from damaged or destroyed devices. Forensic computer analysts must be sensitive to the security concerns of their employers or clients and follow closely all privacy procedures when dealing with financial and personal information. They must also keep detailed and accurate logs and records of their findings, which are often used in litigation.

Education requirements

Employment as a forensic computer analyst normally requires holding a bachelor's degree in computer security, forensic computing or a related subject. Previous experience may also be necessary.

Source: Payscale.com



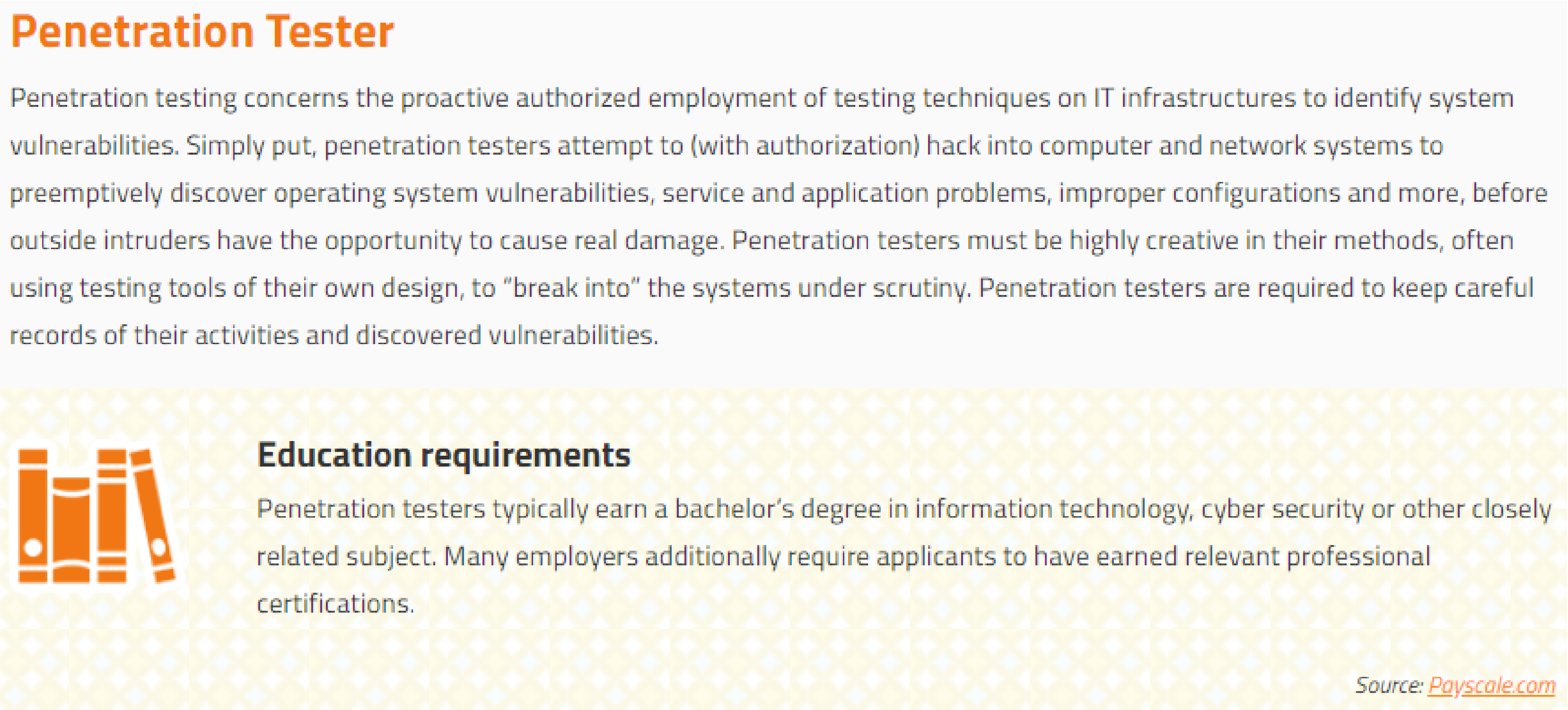
Information Security Analyst

An information security analyst (ISA) is responsible for the protection of an organization's computer systems and networks. They plan and execute programs and other measures, including installing and using software for data encryption and firewalls. Additionally, ISAs help design and execute plans and methods for the recovery of data and systems following a cyberattack. ISAs must continuously stay on top of the latest industry trends and cyber threats, which involves researching new security technologies and networking with other professionals.

Education requirements

ISAs need to earn a bachelor's degree in computer science or related area. There is a growing trend toward undergraduate degree programs specializing in the information security field, which may become the preferred choice of employers in the future. Some employers, particularly large corporations or organizations, may prefer job candidates with an MBA in information systems.

Source: U.S. Bureau of Labor Statistics



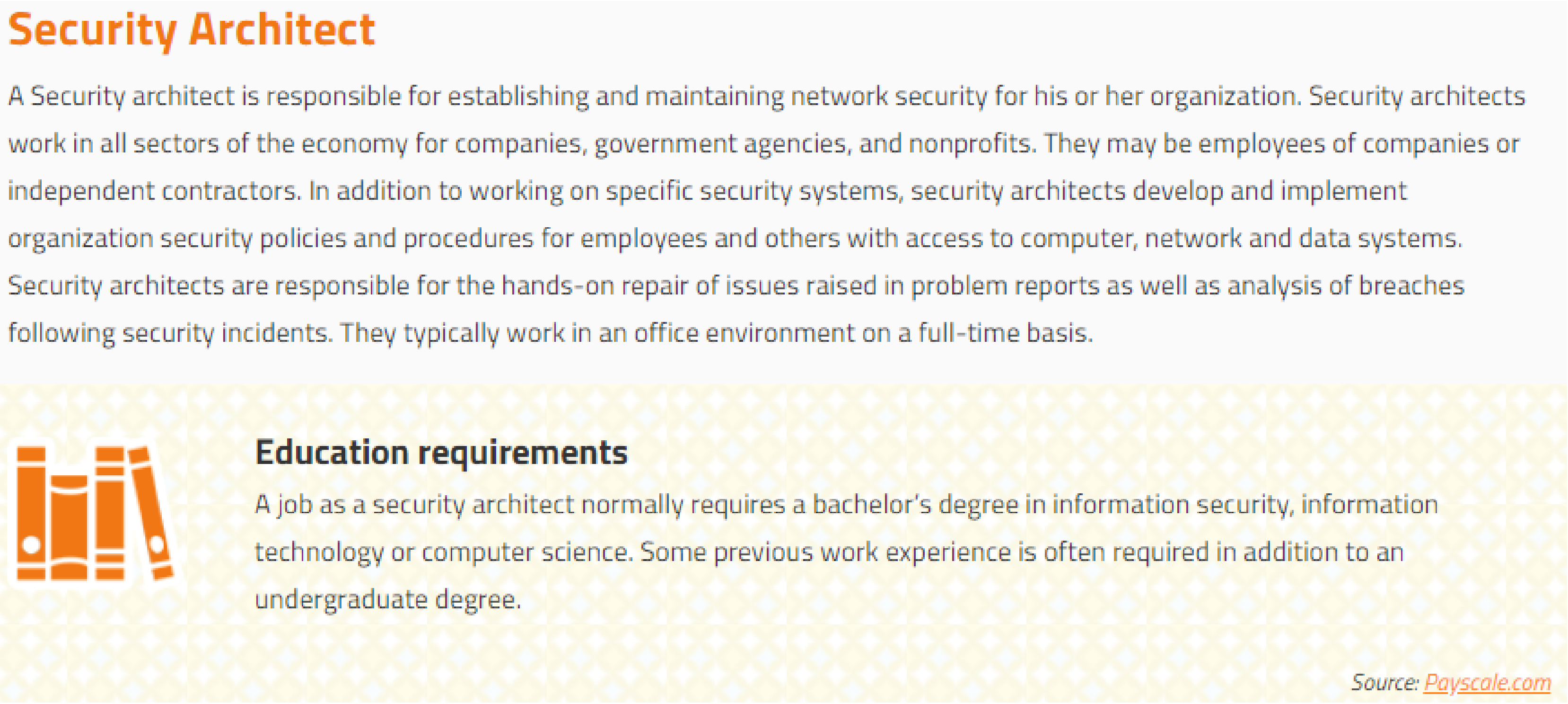
Penetration Tester

Penetration testing concerns the proactive authorized employment of testing techniques on IT infrastructures to identify system vulnerabilities. Simply put, penetration testers attempt to (with authorization) hack into computer and network systems to preemptively discover operating system vulnerabilities, service and application problems, improper configurations and more, before outside intruders have the opportunity to cause real damage. Penetration testers must be highly creative in their methods, often using testing tools of their own design, to "break into" the systems under scrutiny. Penetration testers are required to keep careful records of their activities and discovered vulnerabilities.

Education requirements

Penetration testers typically earn a bachelor's degree in information technology, cyber security or other closely related subject. Many employers additionally require applicants to have earned relevant professional certifications.

Source: Payscale.com



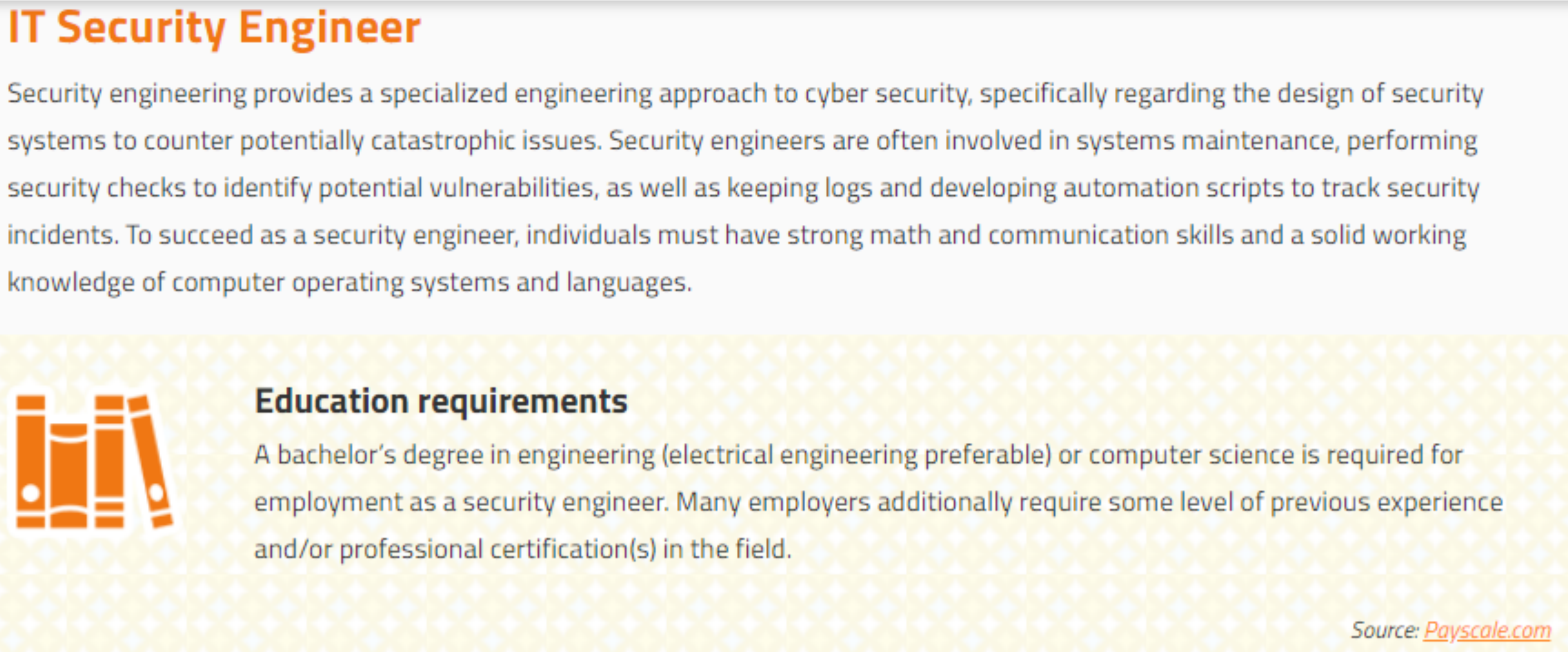
Security Architect

A Security architect is responsible for establishing and maintaining network security for his or her organization. Security architects work in all sectors of the economy for companies, government agencies, and nonprofits. They may be employees of companies or independent contractors. In addition to working on specific security systems, security architects develop and implement organization security policies and procedures for employees and others with access to computer, network and data systems. Security architects are responsible for the hands-on repair of issues raised in problem reports as well as analysis of breaches following security incidents. They typically work in an office environment on a full-time basis.

Education requirements

A job as a security architect normally requires a bachelor's degree in information security, information technology or computer science. Some previous work experience is often required in addition to an undergraduate degree.

Source: Payscale.com



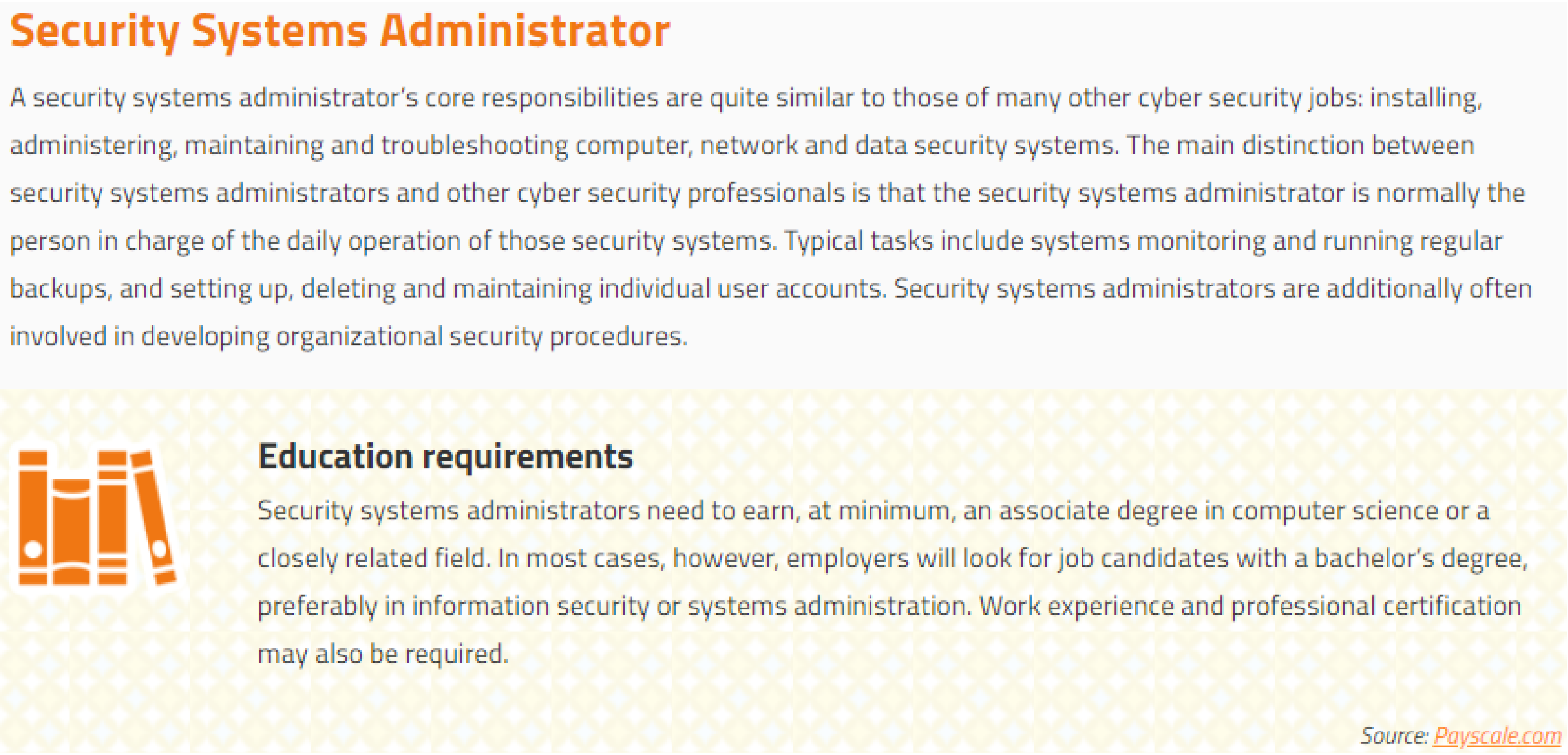
IT Security Engineer

Security engineering provides a specialized engineering approach to cyber security, specifically regarding the design of security systems to counter potentially catastrophic issues. Security engineers are often involved in systems maintenance, performing security checks to identify potential vulnerabilities, as well as keeping logs and developing automation scripts to track security incidents. To succeed as a security engineer, individuals must have strong math and communication skills and a solid working knowledge of computer operating systems and languages.

Education requirements

A bachelor's degree in engineering (electrical engineering preferable) or computer science is required for employment as a security engineer. Many employers additionally require some level of previous experience and/or professional certification(s) in the field.

Source: Payscale.com



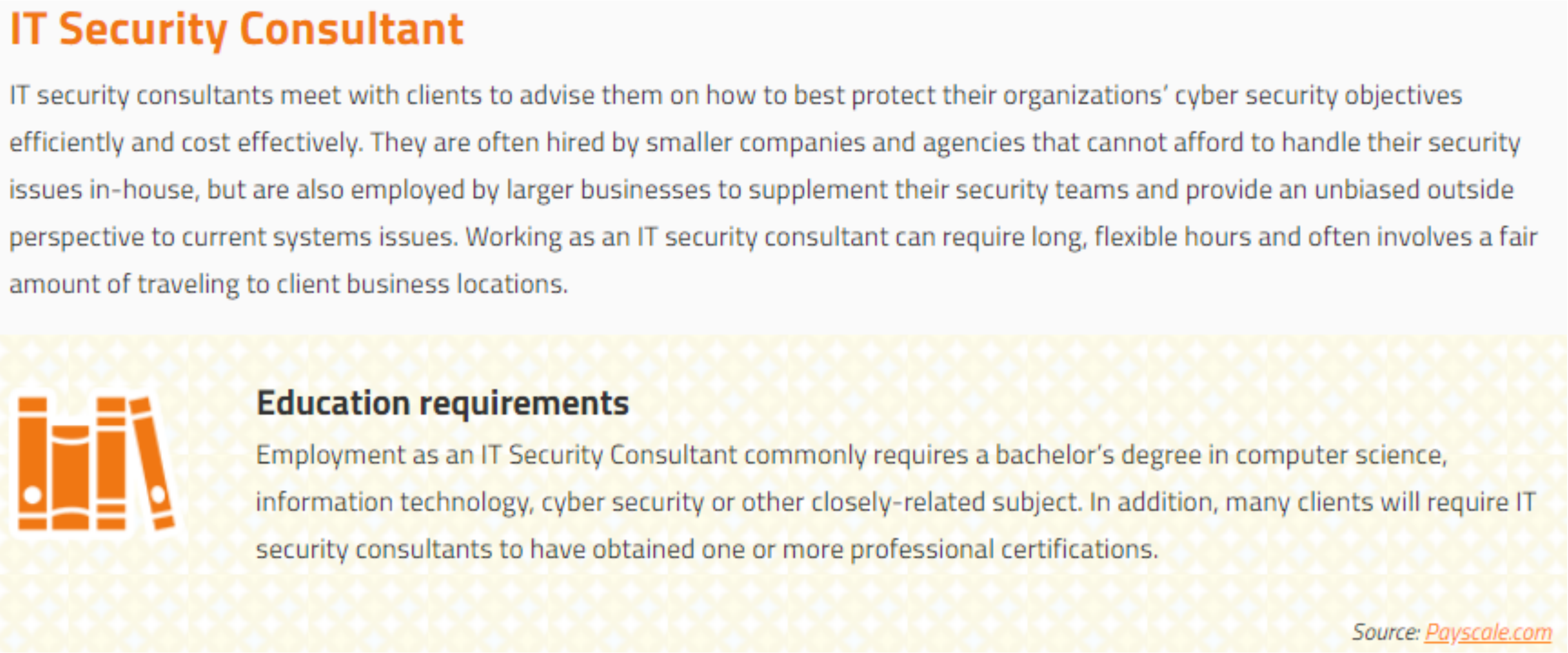
Security Systems Administrator

A security systems administrator's core responsibilities are quite similar to those of many other cyber security jobs: installing, administering, maintaining and troubleshooting computer, network and data security systems. The main distinction between security systems administrators and other cyber security professionals is that the security systems administrator is normally the person in charge of the daily operation of those security systems. Typical tasks include systems monitoring and running regular backups, and setting up, deleting and maintaining individual user accounts. Security systems administrators are additionally often involved in developing organizational security procedures.

Education requirements

Security systems administrators need to earn, at minimum, an associate degree in computer science or a closely related field. In most cases, however, employers will look for job candidates with a bachelor's degree, preferably in information security or systems administration. Work experience and professional certification may also be required.

Source: Payscale.com



IT Security Consultant

IT security consultants meet with clients to advise them on how to best protect their organizations' cyber security objectives efficiently and cost effectively. They are often hired by smaller companies and agencies that cannot afford to handle their security issues in-house, but are also employed by larger businesses to supplement their security teams and provide an unbiased outside perspective to current systems issues. Working as an IT security consultant can require long, flexible hours and often involves a fair amount of traveling to client business locations.

Education requirements

Employment as an IT Security Consultant commonly requires a bachelor's degree in computer science, information technology, cyber security or other closely-related subject. In addition, many clients will require IT security consultants to have obtained one or more professional certifications.

Source: Payscale.com

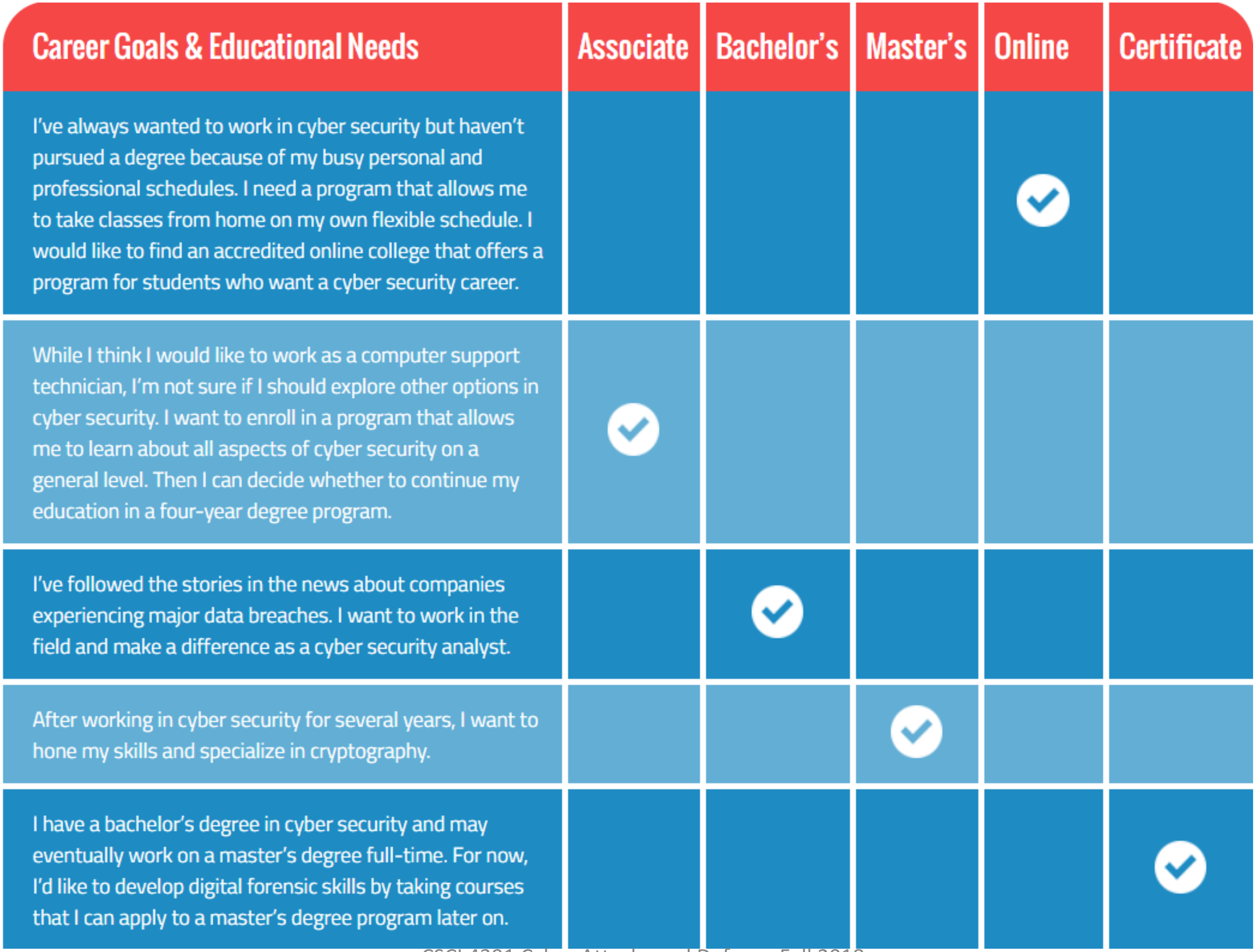
Skills to Acquire

- Communication skills
- Ability to work in a team environment
- Integrity and discretion
- Organization and problem solving skills
- Programming skills
- Understanding of security principles
- Risk analysis
- Network protocols
- Malicious codes
- Intruder techniques

How to Get There?

- Earn a Bachelor's degree:
  - Most position require a four-year degree in cybersecurity or related fields such as CS or IT
- Get advanced training:
  - Advanced degrees such as M.S.
  - Applicable certificates and training
- Obtain security clearance:
  - For applicable jobs

Source: https://www.learnhowtobecome.org/computer-careers/cyber-security/



Career Goals & Educational Needs	Associate	Bachelor's	Master's	Online	Certificate
I've always wanted to work in cyber security but haven't pursued a degree because of my busy personal and professional schedules. I need a program that allows me to take classes from home on my own flexible schedule. I would like to find an accredited online college that offers a program for students who want a cyber security career.				✓	
While I think I would like to work as a computer support technician, I'm not sure if I should explore other options in cyber security. I want to enroll in a program that allows me to learn about all aspects of cyber security on a general level. Then I can decide whether to continue my education in a four-year degree program.	✓				
I've followed the stories in the news about companies experiencing major data breaches. I want to work in the field and make a difference as a cyber security analyst.		✓			
After working in cyber security for several years, I want to hone my skills and specialize in cryptography.			✓		
I have a bachelor's degree in cyber security and may eventually work on a master's degree full-time. For now, I'd like to develop digital forensic skills by taking courses that I can apply to a master's degree program later on.					✓

Certificates

- Top 10 Cybersecurity certificates in 2018:
  - CompTIA Security+
  - CompTIA Advanced Security Practitioner (CASP)
  - Cisco Certified Network Associate (CCNA) Security
  - Cisco Certified Network Professional (CCNP) Security
  - Certified Ethical Hacker (CEH)
  - Certified Information Systems Auditor (CISA)
  - Certified Information Security Manager (CISM)
  - Certified Information Systems Security Professional (CISSP)
  - Certified Cloud Systems Professional (CCSP)
  - Certified Secure Software Lifecycle Professional (CSSLP)

Professional Organizations

- Here is a list of many cybersecurity related industry organizations:
  - (ISC)^2-International Information System Security Certification Consortium
  - The SANS Institute
  - OWASP-The Open Web Application Security Project
  - ISSA-Information Systems Security Association
  - …