Start Engineering

CYBERSECURITY CAREER GUIDE

Prepare for today’s hottest career—become a cyber warrior!

LEARN ABOUT: Types of jobs, where and what to study, salary info, and more.
cybersecurity is

A Great Career Option!

Are you into...Computers and video games? Solving puzzles and mysteries? Writing code and programming computers? Tracking criminals? Defending our country?
Then, cybersecurity could be for you! Because CYBERSECURITY IS...

Defending Our Nation

Cyber criminals, terrorists, and host nation states pose serious challenges to maintaining an open and free society—our way of life—in the digital era. Chinese agents stole U.S. government employees' records from the Office of Personnel Management—a feat North Korea successfully penetrated U.S. and South Korean top secret plans, while Russia interfered in the 2016 presidential election in numerous ways. In addition, national security is affected by criminal assaults on the IT systems of financial institutions and other major businesses too numerous to list. The U.S. Intelligence Community (IC) is beefing up our capability to confront these serious and evolving threats. The IC is coordinated by the Office of the Director of Intelligence and includes the CIA plus a large group of agencies within the Department of Defense—such as the U.S. Cyber Command, Justice, Homeland Security, and Treasury. It's a real-time, round-the-clock, highest-priority effort.

Safeguarding Telecommunications

Because the telecommunications industry builds, controls, and operates the nation's critical information infrastructure, these businesses are inviting targets for both cyber criminals and foreign adversaries. When Verizon, the largest U.S. mobile phone and Internet service provider, announced that 14 million customers were exposed to a security breach, it was a familiar tale of woe: AT&T and several smaller telcos had also been attacked. Access to customer data opens the door to individual identity theft and corporate blackmail. In addition to protecting consumers' stored information, telecom companies must protect leased equipment, such as routers, that both individuals and businesses depend on.

Securing Our Money

U.S. banks and investment institutions are potential treasure troves of personal data and money. In recent years, financial services powerhouse JP Morgan Chase had a breach that affected tens of millions of people and seven million businesses. Cyber criminals find holes in software, penetrate information systems, and install their own codes. They target email accounts to steal passwords for bank and credit card accounts (phishing). They also target websites to infect them with malicious software (malware) or programs that lock users out of their own IT systems to force payment for getting sites and systems back (ransomware). And, just recently the U.S. Secret Service warned about "judging" or "jacking"—a sophisticated crime in which thieves install malicious software and/or card skimmers at ATMs that force the machines to spit out huge volumes of cash like a Vegas slot machine.

CYBERSECURITY FIELD AVERAGE STARTING SALARY: $75,484*

*Data from U.S. Military Intelligence Community Source: Department of Homeland Security

Protecting Our Electric Grid

Imagine you can't charge your iPhone or get that Xbox up and running. Think of life-support machines in hospitals shut down. That's just what could happen if the U.S. electric power grid comes under a cyber attack. In 2016, one-third of Ukrainians lost all electricity in a Russian cyber attack. Today's foreign state competitors and adversaries—Iran, North Korea, and China, as well as Russia—are all devolving cyber tools to cripple this increasingly computerized and interconnected U.S. electric grid: a shocking possibility.
cybersecurity is

Keeping Retailers in Business

While retailers like Target and Home Depot capture the headlines when it comes to cyber attacks due to the volume of the stolen credit card data, the Cisco 2017 Annual Cybersecurity Report makes clear that the entire industry is under continuous attack. Nearly one in three retailers has sustained revenue loss due to cyber attacks. Ironically, because retailer boast revenues by improving operations with technology, so are they exposing themselves and their customers to theft. Both Main Street shops and Big Box stores face the same challenge of keeping information shoplifters out of their cyber space.

Deterring Industrial Espionage

The typical corporate spy used to be a rogue employee with a briefcase, spiritoual paper records of the trade secrets he had personal access to for sale to a rival competitor. Technology raised the stakes, and corporate espionage has only become more menacing with IT development. Today, the information systems of global corporations contain intellectual property worth billions of dollars and essential to a nation’s competitiveness and defense. All of it is at risk, not only from disgruntled employees but also from organized crime and foreign competitors and adversaries. According to General Keith Alexander, the former Commander of the U.S. Cyber Command, “the loss of industrial information and intellectual property through cyber espionage constitutes the greatest transfer of wealth in history.” It is also a major security risk.

Maintaining Medical Confidentiality

Not so long ago, hospital records were on paper locked in file rooms. To day, most hospital records are digitized and locked in IT systems. Electronic record keeping creates efficiencies, particularly in the exchange of information between providers and insurers. But it has also exposed hospitals and their patients to a variety of risks. According to reports, during 2016 there was at least one health-related data breach per day— affecting a total of more than 70 million patient records. Hackers can commit insurance fraud with stolen health data as well as identity theft. Also, using ransomware, hackers have held hospitals’ data hostage, risking hospital services and potentially patients’ lives. Without investment in cybersecurity, the health industry could face a hacking pandemic.

Driving Improvements

Imagine a world in which overtired, distracted, and drunk drivers don’t exist; highway deaths would plummet! Google, General Motors, Tesla, and other major car manufacturers are racing to ramp up production of driverless cars, so that by 2020, America can start to reap the benefits of this exciting new technology. But before the driverless car industry can hit the road, it needs to address the threat of cyber attacks. A computer-driven car connected to a satellite GPS technology is a target as much as transport. Just a few years ago, a team of experts hacked the network of a semi-autonomous Jeep Cherokee and killed the transmission. Instantly stopping the vehicle. Now imagine ransomware doing that to you—or to a truck with a cargo of HAZMAT. The market for autonomous vehicles will suffer from smooth without cybersecurity driving development.

DID YOU KNOW?

1. Cybersecurity isn’t just coding and programming. It’s also drafting and implementing cybersecurity policies for secure information exchange and storage. And cybersecurity is digital forensics for finding how who did what, where, and when—in order to stop them in the future.

2. The most important skills for success in a cyber job aren’t necessarily tech-related. Communication skills are commonly seen as being extremely important in cybersecurity. Knowledge of the system is important, but a cybersecurity professional must be able to speak to others about the importance of cybersecurity as well as present an argument to others about why they need to focus on the issue.

3. Women and minorities make great cybersecurity experts because they tend to come from diverse personal and academic backgrounds and bring broad perspectives to analysis, teamwork, and problem-solving.

SOURCE: KATHERINE BOYER/AMERICAN INSTITUTE OF CIVIL ENGINEERS
There are many options for starting and advancing in careers within cybersecurity. Pick a path that works for you.

To advance further, you'll need an associate's degree or bachelor's degree.

Keep in mind that 83% of job postings ask for a bachelor's degree or higher.
types of careers

Pick Your Path

Cybersecurity professionals are needed in every industry to protect information systems and data from cyber bad guys. But there are many different types of cybersecurity jobs: “ethical hackers” who test IT systems by trying to break into them; analysts who look for evidence of system penetration; forensic analysts who investigate how break-ins occurred; recovery specialists who rebuild and recover data; and managers who organize objectives, lead teams, and report on results. The range of job possibilities is literally awesome.

In 2010, the National Institute of Standards and Technology (NIST) launched the National Initiative for Cybersecurity Education (NICE). NICE embraces the Cybersecurity Workforce Framework, which outlines seven functions or capabilities a cybersecurity system must have: Investigate, Collect and Operate, Securely Provision, Operate and Maintain, Analyze, Protect and Defend, and Over Sight and Develop. Take a closer look at what each of these functions includes on the next three pages. Which interests you most? Because some functions overlap, if you start in one job area, you generally can shift to another with some extra training. But there's no need to decide on a job before looking into paths to skills training and options in higher education—cybersecurity careers start with other certifications or degrees.

INVESTIGATE
Investigate, review, and evaluate cyber events and cyber crimes.

WHAT THEY DO
- Investigate cyber crimes
- Recover data from computers to use in prosecuting crimes, analyzing and decrypting any type of hidden information
- Identify and assess cyber criminals or foreign entities
- Help law enforcement and counterintelligence investigations

JOB TITLE EXAMPLES
- Forensic Computer Analyst
- Cryptographer
- Cyber Intelligence Analyst
- Security Analyst

DEGREE OR TRAINING
- Computer Science
- Network Security
- Information Assurance
- Forensic Science
- IT and Security

SECURELY PROVISION
Conceptualize, design, and build secure IT systems.

WHAT THEY DO
- Create tools for virus, spyware, or malware detection
- Prevent intrusions to computer systems
- Analyze and test computer applications or software
- Technology research and development
- Determine systems requirements and development
- Test and evaluate systems

JOB TITLE EXAMPLES
- Computer Programmer
- Computer Systems Analyst
- Software Developer
- Systems Engineer
- Information Assurance Developer
- Network Security Analyst
- Systems Security Architect
- Information Technology Director

DEGREE OR TRAINING
- Computer Science
- Networking
- Electrical Engineering
- Systems Engineering

COLLECT AND OPERATE
Collect, process, analyze, and present information from adversaries that may be useful to develop intelligence and counterintelligence.

WHAT THEY DO
- Collect intelligence, and interpret and analyze information
- Discover and mitigate criminal and adversarial threats

JOB TITLE EXAMPLES
- Cyber Analyst
- Intelligence Analyst
- Information Systems Manager
- Security Software Developer

ADVANCED DEGREE OR TRAINING
- Cybersecurity
- Computer Science or Engineering
- IT or Network Security
types of careers

OPERATE AND MAINTAIN

Provide support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. Of all the roles, this one has the most job openings.

WHAT THEY DO
- Develop, support, and maintain databases and networks
- Manage intellectual capital and content
- Install, configure, test, operate, maintain, and manage network server configurations, access, firewalls, and patches

JOB TITLE EXAMPLES
Customer/Technical Support Specialist
Data or Database Specialist
Information Systems Security Engineer
Network Security Specialist
System Administrator

DEGREE OR TRAINING
Computer Science
Information Technology
Network Computing Systems

WHO DONE IT?
A digital forensic examiner on an IT system just as a medical examiner at a crime scene. As a digital forensic examiner, a forensic analyst has to be incredibly curious about how computers work and how people behave. In addition to curiosity and insight, you will be expected to have strong written and oral communication skills. A large part of an exam is devoted to deconstructing and explaining evidence. In the case of criminal prosecutions, you will be able to explain your findings before lawyers, judges, and juries who lack tech backgrounds. Can you defend your findings when cross-examined by opposing counsel? Whether you are a non-technical partner, corporate clients, or law enforcement, you need to be able to communicate clearly.

ANALYZE

Responsible for expert review and evaluation of incoming cyber security information to determine its usefulness for intelligence.

WHAT THEY DO
- Identify and assess the capabilities and activities of cyber criminals or foreign entities
- Produce findings to help inform or support law enforcement and counterintelligence investigations or activities
- Analyze threat information from multiple sources, disciplines, and agencies across the intelligence community

JOB TITLE EXAMPLES
Ethical Hacker
Incident Responder
Penetration Tester
Intelligence Analyst
Security Analyst
Overhead Information Security Officer

DEGREE OR TRAINING
Computer Science
Cybersecurity
Information Assurance
IT and Security
Network Security

PROTECT AND DEFEND

Identify, analyze, and prevent cyber threats to an organization.

WHAT THEY DO
- Look for weaknesses in your software, hardware, and networks and find creative ways to protect it
- Respond to incidents
- Manage and monitor networks to remediate unauthorized activities
- Conduct assessments of threats and vulnerabilities

JOB TITLE EXAMPLES
Ethical Hacker
Incident Responder
Penetration Tester
Intelligence Analyst
Security Analyst
Overhead Information Security Officer

DEGREE OR TRAINING
Computer Science
Cybersecurity
Information Assurance
IT and Security
Network Security

CALLING ALL (ETHICAL) HACKERS

A penetration tester (aka, ethical hacker) is a pen tester who attacks computer systems to exploit vulnerabilities. In web-based applications, networks, and systems, in other words, you’re paid to hack — and it’s legal! Using a series of penetration tools, some tools that you will design yourself, if you simulate real-life cyber attack, perhaps taking part in Red Team/Blue Team exercises that mimic cyber warfare. Your ultimate aim is to help an organization improve its cybersecurity. Most pen testers don’t hold a special degree. Since ethical hacking is more about skills than covers letters, a bachelor’s or associate in cybersecurity may be unnecessary if you have the right experience.

OVERSIGHT AND DEVELOPMENT

Provide leadership, management, direction, and/or development and advocacy so that individuals and organizations may effectively conduct cyber security work.

WHAT THEY DO
- Offer legal or policy advice
- Manage the technical direction and strategic plan for an organization
- May include e-commerce, privacy, copyright, and intellectual property

JOB TITLE EXAMPLES
Chief Information Officer
Cyber Security Trainer
Lawyer or Legal Advisor
Policy Analyst

ADVANCED DEGREE OR TRAINING
Business Administration
Criminal Justice
Information Technology
Law
Get Ready: 7 Things To Do Now
Making smart decisions in high school will pay off later.

Given the increasing number, diversity, and complexity of information systems, cybersecurity is one of the most exciting career areas out there. Any cybersecurity career requires a credential or degree of some kind, but there are two-year, four-year, and graduate school possibilities, as well as certifications and higher education online. Rather than sweat those details now, take these steps in high school to keep your options open.

1. Take plenty of math classes. As far as preparation goes, the first and last word is math, so cover algebra, through calculus, to the highest level possible. Does your school offer computer science or statistics? If you can, take these courses, but prioritize the fundamentals, including physics.

2. Don’t shelve English. Keep writing and critical thinking classes like social studies in your school schedule because you’ll need to be able to communicate all your great ideas.

3. Learn basic coding. If your school doesn’t offer coding classes, there are FREE online computer science and coding classes (see page 23 for more information). Check out Code Academy, Alison.com, and Khan Academy. Or enroll in online courses with a for-profit college.

4. Build your own website. Once you have a basic knowledge of coding, build your own site by yourself or with friends to gain experience and programming. You could even try building a home computer network.

5. Go for an internship. As Dr. Margaret Leary of Northern Virginia Community College observes, most cybersecurity careers require working independently but as part of a team, using skills best learned by doing. Colleagues — and employers — look for participation on robotics teams and in computer and cybersecurity competitions, like CyberPatriot (see page 20). If your school lacks these, resources such as NINJALabs and Hour of Code offer online communities for games and competitions. Start an cyber club at your school if there isn’t one. Engineering organizations like the Institute of Electrical and Electronics Engineers (IEEE) Computer Society can help direct you to a local mentor. Local colleges and universities often host activities for high school students interested in computer science and cyber careers, so contact them directly and ask your school counselor to help.

6. Use summer for cyber. A bad job that has you working with computers and solving by security rules beats your college resume. A simple online search will help you find internships and computing skills camps near you. The National Security Agency (NSA) runs the GenCyber Camp program, which is based at colleges nationwide. And if one of those options works for you, those free online activities you didn’t have time for during the school year will fit into any summer schedule at the NSF’s game Day of Cyber mimics a day in the life of a cybersecurity professional in just 2-3 hours.

7. Be good. Whatever else you do, whether in or out, avoid unethical computing and social media activities. Or anything unethical, for that matter. Cybersecurity professionals operate in the most sensitive areas of government and private industry, for which security clearances are required. You need to demonstrate integrity and good judgment, not just good skills.
Four Years of Cyber

A cyber degree at any of the nation’s universities is a great investment in your future.

You’ve decided you want to head straight for a bachelor’s degree, so what is there to know about college and university programs in cybersecurity?

A cybersecurity degree is a Bachelor of Science in a program that combines computer science or similar engineering coursework with classes that develop computing skills. This degree prepares students to analyze the structure of a computer system on an ongoing basis, looking into whether it has been compromised, and eliminating vulnerabilities. Being able to do this depends as much on having computing skills as on knowing the underlying computer science. So in looking for a cybersecurity program, look for programs with coursework and labs in both science and skills, together with extracurricular opportunities for competitions and also internships that develop practical experience.

The National Security Agency (NSA) has accredited college and university programs as National Centers of Academic Excellence in Cyber Operations, CAE-CO. These schools offer cybersecurity degree programs that include coursework in science and engineering, the technology of cyber operations, and additional cyber-learning activities. Because the federal government is the largest employer of cybersecurity professionals, it makes sense that many schools in Maryland and Virginia are CAE-CO accredited. But CAE-CO programs are found in public and private colleges and universities literally all over the U.S. And programs not CAE-CO designated are equally recognized by employers and graduate schools, provided they cover the combination of course work and extracurricular activities offered by CAE-CO programs.

It is obvious that cybersecurity is critical in intelligence and defense. Yet because cybersecurity is also important to healthcare and finance industries, commerce and other business activities (see pages 4-11), degree programs all over the country have developed courses for coursework and research — and partnerships with employers. The University of Southern California offers a degree in Silicon Valley, as well as the defense industry. George Mason University’s cybersecurity program is taught at the George Mason University Fairfax campus. The University of Virginia offers programs in cybersecurity and criminal justice courses, with the goal of joining the Internet Crime Against Children Task Force. Digital forensics is a vital element in law enforcement, answering the what, who, and how questions in computer-based crime, to figure out what happened, apprehend those responsible, and prevent future abuses. Business perceives itself as good at computers, but not really interested in programming. Champlain, in Vermont, and among the top universities in cybersecurity education offers labs to develop hands-on skills in criminal investigations based on actual past cases. And the Lahey Center for Digital Investigations is
SCHOOLS WITH CYBER DEGREES

The schools below offer four-year undergraduate cyber security degrees, or computer science degrees with a cyber security focus. Another option would be to check out engineering schools that offer computer engineering degrees. Other schools offer a minor or certificate in cyber security. You could also take classes online.

So go to this website to find out more: cyberdegrees.org/listings/bachelors-degrees-online/

ALABAMA
Jackson State University
Tuskegee University
University of Alabama at Huntsville
University of South Alabama

ARIZONA
Arizona State University
Embry-Riddle Aeronautical University
University of Advancing Technology

ARKANSAS
Southern Arkansas University

CALIFORNIA
California State Polytechnic University, Pomona
California State University, Sacramento
California State University, San Bernardino
Mt. Sierra College
National University
San Jose State University
University of California, Irvine

COLORADO
Colorado School of Mines
Colorado School of Mines-Pueblo
Colorado Technical University
Unite of State Air Force Academy
University of Colorado, Colorado Springs

CONNECTICUT
Central Connecticut State University
University of Connecticut
University of New Haven
Western Connecticut State University

DELAWARE
Wilmington University

DISTRICT OF COLUMBIA
George Washington University

FLORIDA
Daytona State College
Embry-Riddle Aeronautical University, Daytona Beach
Florida Atlantic University
Florida Polytechnic University
Florida State University
Hodges University
Indian River State College
Keller University
Palm Beach State College
Saint Leo University*
University of Central Florida
University of Florida
University of South Florida
University of West Florida

GEORGIA
Armstrong State University
Augusta University
Columbus State University
Georgia Regents University
Kennesaw State University
Middle Georgia State University
University of North Georgia

HAWAII
University of Hawaii, West Oahu
University of Hawaii, Manoa

IDAHO
College of Western Idaho
Idaho State University

ILLINOIS
DePaul University
Illinois Institute of Technology
Illinois State University
Lewis University
Northwestern University
Southern Illinois University Carbondale
University of Illinois, Urbana-Champaign

INDIANA
Indiana University
Purdue University
Purdue University-Calumet

IOWA
University of Dubuque

KANSAS
Fort Hays State University
Kansas State University
Pittsburg State University

KENTUCKY
Eastern Kentucky University
Kentucky State University
Sullivan University

LOUISIANA
Louisiana Tech University
Southeastern Louisiana University
New Orleans University

MAINE
Thomas College
University of Maine, Augusta
University of Maine, Fort Kent

MARYLAND
Bowie State University
Capital Technology University
Frostburg State University
Morgantown University
Towson University

MASSACHUSETTS
Bay Path University
Boston University
Massachusetts Institute of Technology
Northeastern University
Randolph College
University of Massachusetts Amherst

MINNESOTA
Lake Superior College
Metropolitan State University
St. Cloud State University

MISSOURI
Avila University
Fort Hays State University
Kansas State University
Missouri State University

MONTANA
Montana Tech University

NEBRASKA
Bellevue University
University of Nebraska, Omaha

NEVADA
University of Nevada, Las Vegas

NEW HAMPSHIRE
Southern New Hampshire University

NEW JERSEY
Fairleigh Dickinson University
Felician College
New Jersey City University
New Jersey Institute of Technology
Rutgers, The State University of New Jersey

NEW MEXICO
New Mexico State University

NEW YORK
Beekmantown College
Excelsior College
Hildene College
Iona College
Mercy College
New York Institute of Technology
New York University
 Pace University
Rochester Institute of Technology
St. John’s University
Siena College
SUNY at Albany

OHIO
Lehman College
Ohio University

OKLAHOMA
Oklahoma Baptist University

OREGON
George Fox University
University of Oregon

PENNSYLVANIA
Swarthmore College

RHODE ISLAND
Johnson & Wales University

SOUTH CAROLINA
Lenoir-Rhyne College
University of South Carolina-Upstate

SOUTH DAKOTA
Black Hills State University

TENNESSEE
Fordham University

TEXAS
Our Lady of the Lake University
Texas A&M University
Texas A&M University-Corpus Christi
Texas A&M University-San Antonio
University of Texas at Austin

UTAH
Brigham Young University

VERMONT
Champlain College

VIRGINIA
EDP University
George Mason University
Hampshire College
James Madison University
Marymount University
Norfolk State University
Virginia Tech

WASHINGTON
City University of Seattle
University of Marylhurst

WEST VIRGINIA
Marshall University

WISCONSIN
University of Wisconsin-Stout

*Offers cybersecurity minor or certificate.
Protection Is Their Mission

Companies that provide cybersecurity services to both government and industry can be a great career option.

Cybersecurity companies include organizations that are household names, such as IBM, and companies most of us have never heard of, like Securone Solutions. These businesses provide cybersecurity expertise to government and private industry across a range of functions, from building technology structures to providing personnel for intelligence analysis and counterterrorism. They also have internal needs for information security. These options make for exciting careers.

Cybersecurity companies primarily engage in complex problem-solving in the design and protection of information systems. Every information system has to perform multiple functions. Information exchange is essential to protect the process and ensure verification of those who will access the information. In information storage, it is vital to keep authorized users out. Every day, codes and programs for tracking, preventing, and disabling all kinds of cybersecurity threats are being developed all over the world.

Complex problem-solving demands having teams of professionals with a wide range of skills and backgrounds. Palo Alto Networks in California is among the foremost cybersecurity companies. Senior Director of Information Security Rishi Sebastian says that cybersecurity is the broadest field he knows because any degree can be the basis for a career. Cybersecurity teams include lawyers because navigating legal and policy issues is part of strategic planning. Having executives with expertise in project management is essential for effective cybersecurity. Sebastian says, "I think the biggest challenge is that we don't have enough cybersecurity professionals who are also good at technical skills." But he also notes that cybersecurity is a fast-growing field, with many opportunities for advancement.

Sebastian says he enjoys the job because he makes an impact for good on the world. "Every day," he says, "I feel aware of the connection between what I'm doing and the world out there." Besides the job, he also takes pride in sharing his own story for his career in information security. Sebastian takes seriously the high demand for cybersecurity professionals, and he is active in work for the development of the field. He says his team participates in national cybersecurity competitions. He also was engaged in the Global Cybersecurity Alliance's "CST" initiative with the Girl Scouts of America to create 50 cyber badges, based on cybersecurity education from middle school through high school, which will be available to all scouts starting in fall 2018. The initiative was led by one of the ATA projects, Deena Phutik, Laser Academy for Engagement at NICE, says that the goal is coming up with fun activities to boost kids' tech and thinking skills in K-12.

Palo Alto employees view the badges, but the curriculum, and have trained group leaders. Having opportunities to enable anyone to gain skills, and experience for pursuing a career in cybersecurity big plus for Sebastian.

Requirements for employment with cybersecurity companies vary, but it is not always the same as those for government agencies. This is because in addition to working on projects related to national defense and law enforcement, employees of cybersecurity companies sometimes work at restricted-access government sites. Keep in mind, however, that because cybersecurity companies serve other clients and have other priorities, you may not have all the privileges for employment at a cybersecurity company even if you are not eligible for security clearances.
careers: Work for the Government

Your Country Needs You

With cyber attacks on the rise, protecting and defending in cyberspace is mission-critical.

The federal government is the largest employer of cybersecurity professionals. National defense is an obvious reason why. What sets government apart from private industry is mission, not skills. Military and civilian cybersecurity experts work in intelligence analysis, counter-intelligence, counter-terrorism, and support to special operations. Government careers are also in law enforcement, tracking national and global developments in financial crime, human trafficking, extremist organizations, and more, in order to prevent crime and punish criminals. State and local government law enforcement agencies also employ cybersecurity professionals.

In addition, every government agency manages its own information and records system, and the federal government oversees large repositories of information. Since 9/11, many agencies have been mandated to share information or collaborate in multi-agency task forces. Exchanged information ranges from PI (personally identifiable information) to top-secret intelligence, and it all needs to be kept safe from hack-
**PAYING OFF**
Cybersecurity salaries in the U.S.

<table>
<thead>
<tr>
<th>Job Title</th>
<th>Median Annual Salary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Consultant</td>
<td>$123,885</td>
</tr>
<tr>
<td>IT Security Specialist</td>
<td>$109,366</td>
</tr>
<tr>
<td>Network Security Engineer</td>
<td>$107,931</td>
</tr>
<tr>
<td>Information Security Analyst</td>
<td>$92,600</td>
</tr>
<tr>
<td>Security Analyst</td>
<td>$85,238</td>
</tr>
<tr>
<td>Security Engineer</td>
<td>$81,036</td>
</tr>
<tr>
<td>Intelligence Analyst</td>
<td>$51,605</td>
</tr>
<tr>
<td>Information Technology Specialist</td>
<td>$41,579</td>
</tr>
</tbody>
</table>

**FAST GROWING & WELL PAID**
Jobs for cybersecurity analysts are expected to grow by 28% between now and 2025, with a median annual salary of $92,600.

**JOB OPENINGS IN THE U.S.**
350,000

**WHERE THE JOBS ARE**
Cities ranked by pay for cybersecurity analysts
- Minneapolis, MN
- Seattle, WA
- San Francisco, CA
- Dallas, TX
- Denver, CO
- Chicago, IL
- Austin, TX
- Salt Lake City, UT
- New York, NY
- San Jose, CA
- San Diego, CA
- Washington, DC
- Boston, MA
- Los Angeles, CA
- Arlington, VA

**EQUAL PAY**
Men and women in cybersecurity are paid about equally.

In STEM fields women get paid 93 cents to men’s dollar. All other fields women get paid 77 cents to men’s dollar.

**Start Engineering**
Publisher: Robert T. Black
Creative Director: Stacie A. Harrison
VP, Learning and Communications: Eric Iverson
Editors/Writers: Stacie A. Harrison, Eric Iverson and Catherine P. Lincoln

If you’d like to purchase more career guides, go to: start-engineering.com/shop/
© 2018 by Start Engineering
www.start-engineering.com