



[Career Advice](#) / [Career Paths](#) / [Computer Careers](#) /

# Your Guide to Cybersecurity Careers

Cybercriminals are becoming increasingly sophisticated—but cybersecurity professionals are getting savvier as well.



By Dillon Price, Monster Contributor



With the great power of the Internet comes great responsibility—and potential danger for the businesses that store customer data online. An attack from cybercriminals can bring an organization to its knees, putting sensitive data and assets in jeopardy. That’s why the need for cybersecurity careers is greater today than ever.

In this article, we’ll walk you through the most common cybersecurity roles, how to land a job in cybersecurity, and the salary you can expect from this in-demand career.

## What Does Cybersecurity Do?

Cybersecurity professionals protect information and systems from cyberattacks and data breaches, such as:

- Hacking
- Ransomware
- Malware
- Phishing
- Denial-of-service (DoS) attacks
- SQL injection attacks
- Keylogging
- Email guessing
- Internal threats involving unauthorized access

Most cybersecurity professionals work for computer systems design companies, computer services, financial institutions, information and data management companies, private enterprises, government agencies, and administrative support services. They typically work full-time (sometimes more than 40 hours per week) and may remain on call in the event of an emergency outside of business hours.

## Which Industries Do Cybersecurity Professionals Typically Work In?

It should be no surprise that the industries that get targeted the most by cybercriminals also have a high demand for cybersecurity professionals. Some of the best cybersecurity jobs can be found in these industries:

- Healthcare
- Government
- Finance
- Manufacturing
- Education
- Energy and utility sectors
- Retail

## Is Cybersecurity a Good Career?

The overall cost of cybercrime is expected to reach **more than \$10 trillion** over the next two years, according to a report by Cybersecurity Ventures. That's why the future of cybersecurity is looking bright for job seekers in the tech industry. In fact, **cybersecurity job growth** is expected to increase by 33% over the next decade, according to the Bureau of Labor Statistics.

In fact, there's a major shortage of cybersecurity professionals around the world, with more than **700,000 unfilled positions** in the United States alone. In addition to job security, careers in cybersecurity offer excellent pay and the flexibility to work remotely.

Additional benefits of working in cybersecurity careers include:

- Plenty of opportunities for advancement.
- The ability to work anywhere in the world.
- The opportunity to work with constantly evolving technology.
- Excellent work-life balance.
- The option to become self-employed.

## What Are the Most Common Cybersecurity Career Paths?

Once you've gained the necessary education, certification, and hands-on experience, the career path you'll embark on will likely include these cybersecurity job titles:

- **Entry-level:** Security specialist, security administrator, vulnerability assessor, incident reporter, security consultant, security analyst, ethical hacker, and cryptographer.
- **Mid-level:** Security auditor, security engineer, information security analyst, penetration tester, incident responder, information assurance engineer, and cybersecurity forensic investigator.
- **Senior-level:** security manager, security director, chief information security officer (CISO), and deputy CISO.

Below, we have outlined the most common cybersecurity jobs to consider and which credentials you'll need to apply.

## How to Get an Entry-Level Cybersecurity Job

If you're looking to get your foot in the door, you'll need at least a bachelor's degree in cybersecurity, computer science, information systems, or a related field. Plus, you typically need at least three years of related experience to land an entry-level cybersecurity job. Some cybersecurity professionals start out as **help desk technicians** or **network administrators**.

An internship is also a great way to springboard your cybersecurity career. In an internship, you'll receive cybersecurity job training by performing tasks under the supervision of an

experienced cybersecurity professional. Some internships may eventually allow you to work on security projects independently.

The Department of Homeland Security offers a **10–12 week paid internship program** for high school and college students who have at least a 2.0 GPA.

In a cybersecurity internship, you may do the following:

- Keep track of inbound security data.
- Address and escalate minor security events.
- Test web application security.
- Identify vulnerabilities in network security.
- Research cybersecurity risks and threats.
- Provide penetration testing assistance.
- Debug or disassemble malicious software.

The cybersecurity skills you'll need to succeed in the world of cybercrime include:

- Strong analytical skills.
- Careful attention to detail.
- Excellent problem-solving and decision-making skills.
- The ability to think outside the box.
- Exceptional communication skills.

See our [cybersecurity job description sample](#) to find out what employers are looking for in candidates.

## How to Become a Cybersecurity Analyst

Cybersecurity analyst can be an entry-level or mid-level position. Cybersecurity analysts are responsible for analyzing and monitoring organizations' IT infrastructures for potential cyberattacks or security breaches. Additional responsibilities include:

- Configuring cybersecurity software, password protectors, and other tools.
- Understanding and creating reports that highlight an organization's security capabilities and vulnerabilities, and unusual network activity.
- Testing organizations' networks and identifying and addressing weaknesses.

To land a job as a cybersecurity analyst, you'll need a bachelor's degree (in computer science or a related field) and an understanding of preventative methods, technologies, and threat

detection protocols.

Many employers require you to have about four years of hands-on IT or cybersecurity experience, as well as GSEC and CompTIA Security+ certification. Mid-level cybersecurity analyst positions may require CISSP certification.

Find [cybersecurity analyst jobs](#) on *Monster*.

## Mid-Level Cybersecurity Careers

Once you've got some cybersecurity experience under your belt, you can take on mid-level cybersecurity careers.

### How to Become an Information Security Analyst?

You've likely heard the term before, but what is an information security analyst? An information security analyst is a cybersecurity professional who is responsible for protecting sensitive data, technology systems, and networks. Information security analysts plan, design, and implement cybersecurity solutions to mitigate the risk of data breaches and cyberattacks.

Many employers require information security analysts to have five years of previous cybersecurity experience, knowledge of the [HIPPA Security Rule](#), as well as CISSP, CISM, CEH, and GSEC credentials.

Find [information security jobs](#) on *Monster*.

### How to Become a Cybersecurity Engineer

Most cybersecurity engineer jobs are mid-level positions, while some are entry-level or senior-level. Cybersecurity engineers are responsible for the creation and management of cybersecurity software, hardware, and policies. They're also responsible for designing, implementing, testing, monitoring, troubleshooting, and updating secure network solutions.

As a cybersecurity engineer, you will also:

- Conduct penetration tests.
- Respond to security breaches.
- Assist with security breach investigations.
- Participate in change management.

To qualify for a cybersecurity engineer job, you'll need:

- A bachelor's degree in computer science, systems engineering, or a related field.

- 2-7 years of professional cybersecurity experience, including firewall protection, endpoint security, incident detection, and forensics.
- Proficiency in programming languages such as Java, C++, Python, Node, Ruby, Power Shell, and Go.

Find [cybersecurity engineer jobs](#) on Monster.

## Senior-Level Cybersecurity Careers

Are you a seasoned cybersecurity professional looking to move your way to the top? Below, we'll explore cybersecurity careers in security management, security architecture, and other senior-level positions.

### Sign Up For Newsletters

Create an account and get career advice sent to your inbox!

Continue with Google

Sign Up

**MONSTER**

## How to Become a Cybersecurity Manager

Cybersecurity managers monitor, observe, and manage all operations that occur within a network. They're also responsible for overseeing technological resources, risk mitigation, and overall IT security infrastructures.

Since this is an advanced cybersecurity position, you'll need the CISSP and/or CISM credentials, at least five years of related experience, and excellent leadership and decision-making skills. Some employers may require a master's degree in cybersecurity management before hiring you.

Find [cybersecurity manager jobs](#) on Monster.

## How to Become a Cybersecurity Architect

Cybersecurity architect is a senior position. As a cybersecurity architect, you would plan, design, test, implement, and maintain computer and network security infrastructures. You would also test and analyze organizations' existing cybersecurity capabilities and develop methods, protocols, policies, training, and security measures to address vulnerabilities.

To get a job as a cybersecurity architect, you would first need a bachelor's degree in computer science, cyber security, or a related field—many employers prefer candidates who have a master's degree. Plus, you would need 8–10 years of professional IT or cybersecurity experience. Most employers will require you to have CISSP, CEH, and GSEC certifications.

*Find [cybersecurity architect jobs](#) on [Monster](#).*

## How to Become a CISO

CISOs are responsible for overseeing an organization's (typically a large organization) entire cybersecurity infrastructure, including its frameworks, policies, teams, and procedures. They're also in charge of managing and training security staff, disaster recovery, incident response, and communicating with CEOs, executives, and boards of directors.

To be eligible for a CISO role, most organizations require about 10 years of experience in cybersecurity. About seven of those years should be in a leadership role, such as security manager, security director, and/or deputy CISO (working under the supervision of a CISO).

CISO jobs also require a master's degree in cybersecurity or a related field. This role also requires you to obtain the [Certified Chief Information Security Officer \(CCISO\)](#) credential from the EC-Council. Other certifications typically required for this role include CISSP, CISM, and CISA.

*Find [CISO jobs](#) on [Monster](#).*

## How Much Do Cybersecurity Careers Pay?

Cybersecurity professionals are in high demand, and many employers will pay good salaries to attract and retain talent. Here are the salaries you can expect for the most common cybersecurity careers:

- [Cybersecurity consultant salary](#): \$119,930 per year
- [Cybersecurity specialist/technician salary](#): \$121,193 per year
- [Cybersecurity analyst salary](#): \$117,750 per year
- [Incident analyst / responder salary](#): \$130,881 per year
- [Information assurance engineer / analyst salary](#): \$118,678 per year

- **Cybersecurity manager/administrator salary:** \$129,172 per year
- **Vulnerability analyst / penetration tester salary:** \$117,316 per year
- **Cybersecurity engineer salary:** \$112,454 per year
- **Information security analyst salary:** \$120,360 per year
- **Data security analyst salary:** \$122,015 per year
- **Cybersecurity architect salary:** \$134,190 per year

Your location and experience level will also influence how much you earn in a cybersecurity job. Monster's [Salary Tool](#) can give you insight into the salaries to expect in your area.

## 6 Popular Cybersecurity Certifications

Whether you're applying for an entry-level or senior-level cybersecurity job, you'll likely need some form of certification. Below, we outline six of the most popular certification programs needed for cybersecurity careers.

### 1. Certified Information Systems Security Professional (CISSP)

The [CISSP certification program](#) offered by the Interagency Security Committee (ISC) is the most sought-after credential for cybersecurity careers. The CISSP program prepares you for designing, implementing, and monitoring cybersecurity programs.

To qualify for this program, you'll need at least five years of experience in at least two of eight areas of cybersecurity. These include:

- Asset security
- Security architecture and engineering
- Security operations
- Software development security
- Security and risk management
- Communication and network security
- Security assessment and testing
- Identity and access management

### 2. Certified Information Systems Auditor (CISA)

The Information Systems Audit and Control Association (ISACA) offers the [CISA certification program](#), which demonstrates proficiency in evaluating security vulnerabilities, designing and implementing security controls, and creating compliance reports.



To qualify for the CISA credential, you'll need five years of IT experience (a bachelor's degree in computer science or a related field may be a substitute for one or two years).

### 3. Certified Information Security Manager (CISM)

The [CISM certification program](#) offered by ISACA is ideal for IT professionals seeking a cybersecurity management role. To qualify for the CISM credential, you'll need at least five years of professional IT experience. Two years can be waived with a master's degree in IT management or a related field.

### 4. CompTIA Security+

The [CompTIA Security+ certification program](#) prepares candidates to assess organizational security, and monitor and secure mobile, cloud, and the internet of things (IoT). Participants will also learn response protocol to security incidents and gain an understanding of risk and compliance.

There are no specific prerequisites for this credential. However, it is recommended that you complete the [Network+ certification](#) program and have at least two years of IT experience before taking the exam.

### 5. Certified Ethical Hacker (CEH)

The EC-Council offers the [CEH certification credential](#) for ethical hackers (also known as "white hat hackers") who work for lawful hacking organizations. The program demonstrates proficiency in penetration testing and cyberattack detection and prevention.

To qualify to take the CEH exam, you'll need two years of IT work experience. However, you can bypass the required professional experience if you have completed the EC-Council [ethical hacking course](#).

### 6. GIAC Security Essentials (GSEC)

The [GSEC credential](#) offered by Global Information Assurance Certification (GIAC) is often a starting point for people pursuing cybersecurity careers. When you obtain the GSEC credential, you'll demonstrate proficiency in network security, incident response, cloud security, cryptography, and active defense.

There are no prerequisites for the GSEC exam. However, GIAC recommends that you have some experience in computer networking and information systems before taking it.

## How to Get a Job in Cybersecurity

Even though the cybersecurity job outlook for the coming years is more than good, you'll still need to create a [cybersecurity resume](#) to be considered for jobs. We have tons of resume

hacks, including tips for highlighting **the right skills** (e.g., intrusion detection, programming, vulnerability scanning, etc.).

Sending a cover letter is also a great way to authenticate your skills and professional IT experience when applying for a job. Check out our cover letter samples for **IT professionals** and **computer science majors** to learn how to create your first draft.

Ready to begin searching for cybersecurity careers, including **information security analyst jobs**? The top five most popular cities to find all **cybersecurity jobs** in are:

- **New York City**
- **Chicago**
- **Washington, D.C.**
- **Los Angeles**
- **Atlanta**

## Create Your Profile Today to Secure a Cybersecurity Job

There are tons of cybersecurity careers available for IT professionals like you. Simply **create your profile** on Monster to monitor our site for job opportunities. To help you secure a new cybersecurity position, we'll alert you of new job postings by sending notifications directly to your phone. We also have plenty of career advice articles to help you pinpoint vulnerabilities in your job application.

Was this article helpful?

Get great content like this and **the hottest jobs delivered to your inbox.**

Sign Up Now



Explore **jobs** at **FedEx, Amazon, Google, Uber, Disney, Microsoft, Walgreens, Best Buy, & many more!**

[Check Out New Jobs](#)

BROWSE ADVICE ARTICLES

[Job Search](#)

---

[Career Paths](#)

---

[Resumes](#)

---

## Career Development

---

## Leaving a Job

---

## Interviewing

---

Cover Letters

---

Most Helpful In Career Paths

[Browse Advice](#) →

**CAREER PATHS**

### How to Become a Portfolio Manager

By Venus Gentile, Monster Contributor

**CAREER PATHS**

### Your Guide to New-Collar Jobs

By Martina Mascali, Monster Contributor

**CAREER PATHS**

### 20 Forward-Thinking Companies Offering B Corp Jobs That Matter

By Venus Gentile, Monster Contributor

**CAREER PATHS**

### What a Startup Environment is Like and How to Thrive in One

By Martina Mascali, Monster Contributor

**CAREER PATHS**

### What Are Small Company Benefits and How Can They Impact Your Career?

By Venus Gentile, Monster Contributor

Monster extracted this information from the job description.

 United States (English) ▾

## For Job Seekers

---

## For Employers

---

## Helpful Resources

---

Find us on social media:



Get the Monster App



© 2025 Monster Worldwide

Looking for Monster Cable?

