August 10, 2021

How to Get a Cybersecurity Job

Tags

Introduction

As the cybersecurity workforce gap becomes more acute, forward-thinking organizations are starting to evolve their recruitment and hiring practices. Hiring managers are increasingly open to recruiting and educating candidates without previous cybersecurity or even IT experience, but that doesn't mean the path is always clear for cybersecurity jobseekers.

Organizations and HR departments continue to set unrealistic expectations for cybersecurity hires and look for candidates with a mix of experience, skills and certifications that are extremely difficult to find. "Some 88% of cybersecurity postings specify at least a bachelor's degree or higher, and roughly the same percent demand at least three years of experience," according to a report by Burning Glass Technologies.

This creates a paradox: The bigger the need to fill positions, the tougher it gets to land one. The problem is at least partly self-inflicted, considering that employers tend to focus on finding "All Star" candidates that, for the most part, do not exist. Job postings, descriptions and hiring requirements are often too broad, tend to demand too much from single candidates, place too much reliance on individuals versus resilient team building, and don't necessarily reflect actual, realistic day-to-day responsibilities.

So as a jobseeker – especially if you lack previous cybersecurity or IT experience – it can be a difficult and frustrating task to find your first cybersecurity job. However, if you approach the task with the right plan, you're in a better position to attract the attention of the right hiring manager and an open-minded employer, even if you lack the technical skills most people think of first.

In this guide, we lay out five components to a successful cybersecurity job hunt:

1. Identify a Position That Interests You

2. Stay Current on the Cybersecurity Profession and Industry

3. Find the Right People to Help You

4. Demonstrate Your Relevant Transferrable Skills

5. Show Them Your Passion

These insights are drawn from the ISC2 Cybersecurity Career Pursuers Study.

1. Identify a Position That Interests You

Demand for cybersecurity talent will grow as organizations struggle to protect their critical assets from threat actors around the world. The challenge for jobseekers is to home in on opportunities that match your skills and break through the barriers that employers inadvertently construct for candidates.

Cybersecurity is a broad discipline that attracts people with a diverse set of experiences. It's easy to focus on the technical aspects and believe that lacking an IT background is a dealbreaker for those hoping to enter the field. However, the ISC2 Cybersecurity Career Pursuers Study found that just over half (55%) of participating cybersecurity professionals transitioned from an IT role. Among those who didn't get into cybersecurity via IT, 21% started their careers in another field. 13% got into cybersecurity after receiving a cybersecurity education, and 8% explored cybersecurity on their own.

These findings suggest there are many pathways for professionals to enter the field. If you are excited by the prospect of a cybersecurity career, love to solve problems, want to help people and society, and are excited by the prospect of working in a constantly evolving field, then you already have a lot in common with today's cybersecurity workforce.

As you launch your pursuit, you will find that cybersecurity is not a homogeneous field limited to a handful of roles. Rather, it covers a variety of functions and responsibilities, and is reliant on teams with diverse skills, experiences and ideas. The following organizations offer helpful resources for you to learn about what roles exist in the field that may align with your experiences, career aspirations and interests.

The NICE Framework

The National Institute of Standards and Technology (NIST) breaks down cybersecurity roles into seven broad categories in its National Initiative for Cybersecurity Education (NICE)

Framework. The NICE Framework is a foundational tool many government agencies and large enterprises use to define roles for cybersecurity positions within their organizations. Jobseekers should be familiar with the basic principles of the NICE Framework as many organizations around the world reference it for their staffing strategies and it does provide a broad overview of the types of roles in the field. It is a very robust and technical document, but it is an important reference point when exploring cybersecurity careers.

CyberSeek.org

CyberSeek is a useful resource for exploring jobs that may be a good fit for you, as well as learning more about which jobs are available throughout the U.S. Supported by NIST and administered by Burning Glass Technologies, CyberSeek includes a heat map showing job openings across the United States and an interactive tool, the Career Pathway, with information on career paths and average compensation in cybersecurity. A similar tool is available for Australian jobseekers at CyberSeek Australia.

CYBER.ORG

CYBER.ORG, formerly the National Integrated Cyber Education Research Center (NICERC), is a cybersecurity workforce development organization that targets students with cyber career awareness. The United States Department of Homeland Security (DHS) supports CYBER.ORG through a grant from the Cybersecurity Infrastructure and Security Agency (CISA). CYBER.ORG offers a simplified review of 20 cybersecurity career opportunities through its Cyber Career Profiles.

National Security Agency

The National Security Agency (NSA) offers career development programs that help employees in other fields cross-train for cybersecurity careers.

United Kingdom Cyber Security Council

The U.K. Cyber Security Council is the self-regulatory body for the U.K.'s cybersecurity profession, commissioned by the U.K. government by a consortium of U.K.-based cybersecurity training and membership bodies. Its website provides essential information on the cybersecurity profession: from what cybersecurity is, to how to join the profession, to how to develop your career across its 16 specialties. It includes interactive careers and qualifications route maps to help illustrate the pathways through both.

Additionally, ISC2 research finds a wide array of job titles are held by individuals with cybersecurity responsibilities around the world and with organizations of all sizes. Familiarizing yourself with the common titles and descriptions can also help you narrow down the field for the roles that may interest you the most.

- Application Developer/Tester

- Business Analyst
- Cybersecurity Professor/Educator/Trainer
- DevOps Engineer
- Help Desk Technician
- Information System Security Manager
- Information System Security Officer
- IT Auditor
- IT Director
- IT Manager
- IT Security Director
- IT Security Manager
- IT Specialist
- Network/System Administrator
- Penetration Tester
- Project Manager
- Security Administrator
- Security Analyst
- Security Architect
- Security Auditor
- Security Consultant/Advisor
- Security Engineer
- Security Researcher
- Security Specialist
- Security/Compliance Officer
- Software developer/engineer
- Systems Analyst
- Systems Architect
- Systems Engineer

There is a wealth of “Cybersecurity Jobs” resources available to learn more about these roles,

including:

- **CyberSN** – The cybersecurity staffing and recruiting company has defined 45 cybersecurity job categories
- **Cybersecurity Ventures** – The global cyber economy researcher offers a list of 50 Cybersecurity Titles That Every Job Seeker Should Know About
- **ONGIG** – The job description management software developer has a list of its Top 30 Cyber Security Job Titles [+ Descriptions]

By getting acquainted with all the job categories and roles that fall under the cybersecurity umbrella, you can determine which areas of the profession interest you most. This is a great first step so you can start focusing your job search, prepare to share how your past experiences are relevant for the role and begin to explore skillsets you need to further develop.

2. Stay Current on the Cybersecurity Profession and Industry

Once you've determined how to focus your cybersecurity job-finding efforts, you can move to the next phase of your pursuit strategy: Learning as much as possible about the profession.

If you're serious about the field, make sure prospective employers see your commitment. That means learning about the industry and the language used by cybersecurity professionals. Like any other profession, such as law or engineering, there is a lexicon and in-the-know vernacular you must learn to be conversant on relevant topics. This will enable you to:

- Demonstrate an understanding of the threat landscape by keeping up with news of evolving attack methods
- Articulate the important nuance between threats, threat actors, attacks, breaches and the concepts of risk and risk management
- Keep current with new and existing technologies, tools and practices used to mitigate risk
- Demonstrate knowledge of industry priorities such as the current emphasis on cloud security and top threats like ransomware

Useful ISC2 Resources

- ISC2 Webinars – Live and on-demand webinars explore best practices, emerging threats, new technologies and issues facing the profession

- The ISC2 Online Community – Cybersecurity professionals connect, collaborate, and share knowledge and best practices related to the very broad topic of security
- ISC2 Security Congress – A premier event for cybersecurity professionals at all stages of their careers to learn about emerging threats and best practices

Valuable Sources of Cybersecurity Insights

- The CyberWire is a comprehensive news aggregator of the latest developments, research, trends, breaches and more. Sites like CSO, CyberScoop, Dark Reading, The Daily Swig, Help Net Security, SearchSecurity and SC Magazine provide original reporting on a wide array of news and issues.
- The Cybersecurity & Infrastructure Security Agency (CISA) offers its National Cyber Awareness System to keep the public aware of active threats
- The Verizon Data Breach Report is one of the world's definitive annual reports on the state of the global threat landscape
- Security vendors, analysts and consultants such as Accenture, Booz Allen Hamilton, Cisco, Deloitte, FireEye, Forrester, IBM, Infosys, McAfee, Trend Micro and others offer in-depth analysis, research and reports on emerging threats and issues
- Security vendors like Bitdefender, CrowdStrike, Digital Guardian, ESET, IBM, Malwarebytes, McAfee, Recorded Future, Symantec, Sophos, Trend Micro, TripWire, Varonis and many more offer commentary on breaking news, threat analysis and exploration of a wide array of security trends. There are also many independent cybersecurity thought leaders publishing their insights and investigations, including Krebs on Security and Graham Cluley.
- There are plenty of cybersecurity podcasts available to explore a wide array of topics and hear the opinions of leaders in the field

Absorb as much information as you can about the roles and responsibilities associated with the job titles that excite you most. That way, once you get in front of a recruiter or hiring manager, you can:

- Ask questions and share opinions that demonstrate knowledge of the profession, as well as the current threat landscape
- Emphasize an understanding of the skills necessary to mitigate risk, such as problem solving, communication and critical thinking
- Show a willingness to learn as much as possible about cybersecurity through training, mentoring, on-the-job learning, webinars and self-guided online courses

The cybersecurity profession and the threats it faces are constantly evolving. Demonstrate

your passion for learning and building greater awareness.

3. Find the Right People to Help You

As a jobseeker, you can't force anyone to hire you. But with the right strategy to market your skills, demonstrate an understanding of the job and convey a willingness to learn and expand your competencies, you can boost your chances of getting hired. Identifying the right people who can help you is an important part of cybersecurity job hunting.

For an outsider trying to break into the cybersecurity field, persistence is a must. If you believe you're right for the job, and possess transferrable skills, don't give up if your first few attempts to get in front of a hiring manager are unsuccessful. While employers may have ideal candidates in mind to fill positions, in many cases it's possible "they don't know what they don't know."

Part of your mission is to reset employer expectations. A hiring manager who is acquainted with the realities of the job market is likely to be realistic about the level of qualifications currently available. As such, they may be more willing to consider you than an HR department's resume-screening algorithm.

Avoid getting discouraged by a negative – or lack of – response from HR. Keep in mind that HR recruiters may be focused on processing applications and candidates across an entire organization. Your goal is to reach the hiring manager. Be determined. Be creative.

Before responding to job postings, learn as much as possible about the employer. Visit the company's website to learn about the organization. Get information through blogs, press releases, annual reports, customer testimonials, and the company's social media presence. Learn about how the company is growing and its plans for the future. Securing those operations and future investments will be critically important, so you should inquire and ask relevant questions during any interviews or even introductory communications.

Scour online communities like LinkedIn to identify members of the security team and likely hiring managers. See if any of those individuals are members of professional organizations or any nearby cybersecurity chapters where you may be able to establish a connection and introduce yourself. You may not be ideal for a current role but building your professional network will pay dividends. Try to make connections outside of the standard HR-centric resume submission. Start building your network of advocates who know you.

Before contacting the hiring manager, consider seeking out cybersecurity team members for information about the field and advice on landing a job. Information shared by a team member could help you prepare for an interview or encourage you to pursue an avenue – such as attending a webinar or conference – that you hadn't yet considered.

The following are exceptional resources for connecting with cybersecurity professionals and other career hopefuls to meet people, discover employers, stay motivated, find inspiration and identify ways to make yourself a more attractive candidate.

Cybersecurity Chapters

There are local chapters around the world that focus on creating in-person and online engagements for cybersecurity professionals. These forums focus on professional development and networking, and many jobseekers will find professionals who are willing and eager to share their experiences and advice. A good place to start is to see if there are any chapters near you from ISC2, ISACA or CompTIA.

Online Communities

If you prefer to engage online, there are many helpful and active forums across social media, including Reddit, LinkedIn and more where you can connect, research your questions and learn from others' experiences and opinions.

Follow Influencers

In addition to joining and participating in online communities, make sure you get a sense of what cybersecurity influencers and thought leaders in the industry have to say. Cybersecurity can sometimes feel like a small community and many professionals are dealing with similar issues. Follow the right people to make sure you're aware of what's driving today's security discussion. If you're just starting your journey, follow people like Cybersecurity Meg for encouragement and helpful insights.

Attend industry events

Cybersecurity conferences provide networking opportunities to get in front of the right people, be it recruiters, hiring managers or cybersecurity team members who can help open doors into their organizations.

Apply for an internship

Internships provide a tried-and-true entry point into a profession and cybersecurity is no different. If you're a college student or recent graduate, seek help from professors and advisors with connections to hiring companies.

Consider the public sector

Government programs such as the National Security Agency (NSA) offer career development programs that help employees in other fields cross-train for cybersecurity careers.

Internal search

If you'd like to transition to a cybersecurity role within your current organization, you may find that you'll have an easier path than you may think. You already understand your organization's work and culture and may have insights into how data flows through systems and controls already in place. These could all be invaluable assets for any member of the cybersecurity team, and candidates may find a willingness for security teams to invest in training you for a new role.

If you have a specific job in mind, learn whatever you can about the role before contacting the hiring manager. By doing research upfront, you can demonstrate knowledge about the position and your seriousness about the job. If no job openings are currently available, ask the hiring manager about potential future opportunities. Also, ask about the availability of mentorships, apprenticeships or job shadowing that can help prepare you for an eventual opening. Gaining experience in your current organization is another pathway to a future cybersecurity career.

4. Demonstrate Relevant Transferrable Skills

As a cybersecurity jobseeker with no experience in the field, you need to envision and articulate how your background can relate to the job and its associated tasks and responsibilities. You may not have had formal technology training, but research shows that cybersecurity professionals rank creativity, analytical thinking and problem solving as key attributes for success in the role.

You've likely had to overcome challenges by uncovering and correcting root causes to issues. Don't discount your experience outside cybersecurity. You have acquired skills that are transferrable to a cybersecurity role. Consider these examples:

Law Enforcement

Experience in forensics and criminal investigations is applicable to investigating and solving cybercrimes and identifying patterns and common targets.

Military

Intelligence-gathering and structured, methodical approaches to challenges are key skills to identifying threats, their origins and their likely targets.

HR

A background in crisis management is helpful when cybersecurity teams must respond to attacks. Experience with policy writing and communicating sensitive information can be used to train users on cybersecurity practices and explain cybersecurity policies to them.

Legal

Knowledge of compliance requirements for regulations on privacy, data sovereignty and cybersecurity is extremely valuable in setting cybersecurity policies and ensuring compliance with relevant laws.

Accounting, Finance and Insurance

Experience with risk analysis and sorting through large volumes of data is transferrable to assessing cyber risks and working with machine learning (ML) models trained to sift through data for anomalies.

Marketing

Digital marketers today must understand the flow of data, sound governance of data, adherence to a wide array of privacy regulations, systems architecture and more, as well as bringing a creative mind to complex and technical challenges.

Non-Technical Skills

Soft skills? There is nothing soft about non-technical skills. They are absolutely critical in cybersecurity roles, and sometimes they are harder to teach and learn than technical know-how. Consider this comment from a cybersecurity professional in the Pursuers Study: “The soft skills and ability to articulate and implement requirements helped me a lot.” This respondent was not alone; the value of non-technical skills was a recurring theme in the study, with professionals citing the importance of skills such as creativity, problem solving and analytical thinking.

Here is a complete list of non-technical cybersecurity skills that professionals say are most important to success:

1. Analytical Thinking

2. Problem Solving

3. Critical Thinking

4. Ability to Work in a Team

5. Creativity

6. Ability to Work Independently

7. Data Visualization

8. Business Acumen

9. Leadership

10. Project Management

11. Verbal Communication

12. Written Communication

Don't sell yourself short. Be sure to emphasize these skills and the experiences in which you put them to work to make you an attractive candidate to a cybersecurity team leader. Don't just offer a bland list of past employment in your resume. Speak to your problem solving, tenacity and ability to find creative solutions to new problems.

If You're Currently in IT

If you work in IT, or have done so in the past, your path to cybersecurity may be more direct. 55% of current cybersecurity professionals in the Pursuers Study transitioned from IT. This isn't surprising since IT and cybersecurity involve many similar tasks such as configuring, deploying, managing and monitoring systems. Be sure to highlight this experience, whether you are applying for a job internally or elsewhere. But also, be aware that – as explored above – cybersecurity is more than a technical discipline. If you have a predominantly technical background, make sure you express all your security experience, but also focus how you applied your knowledge to enable operations efficiently and securely.

The same goes for cloud experience. If you have it, play it up, because it is a distinct advantage. Cybersecurity professionals polled in the Pursuers Study deemed cloud security to be the most important technical concept to understand in pursuing a cybersecurity position. Most environments currently are hybrids that mix on-premises infrastructure with public and private cloud services.

Diversity

Forward-thinking organizations and cybersecurity teams recognize that differences in culture, experiences, languages and backgrounds can add fresh thinking and creativity in solving problems and completing tasks. Often, employers are unsure how to go about making their teams more diverse, but you can help them by pointing out how you bring a unique or fresh perspective to the organization. Make it clear how your addition to a team could help broaden awareness and bolster the human side of cybersecurity. Can you understand the mindset and motivation of threat actors from specific countries or regions? Are you familiar with how different cultures and age groups learn to bolster the user awareness trainings in global organizations? Do you speak another language? Have you had to engage with international colleagues or clients? Think broadly and creatively about how your background can be applied and be an asset for your future team.

5. Show Them Your Passion

Experienced hiring managers know to look for a variety of attributes when reviewing candidates for cybersecurity positions. One important attribute has little to do with technical prowess or other skills. It's passion. If you can demonstrate passion and commitment to the job, a good hiring manager will pick up on it. Explain how you used your passion and commitment to learn in the past, and how you would apply the same level of dedication to learning new skills to succeed in cybersecurity.

Make it clear you are motivated by the opportunity to work on a team and solve the problems that have become one of modern society's greatest ills – cyberattacks. Being able to work in an uncertain environment where crisis is always a possibility isn't for the faint of heart. And you don't do it just for the compensation. You do it so you can make a difference and enjoy the rewards of performing in a relentless, high-pressure environment.

When asked about their experience in cybersecurity, current professionals talk about the challenges they faced. But what often rises to the surface is their passion for the job, their love of learning how to solve problems and overcome challenges, and the perseverance it takes to succeed.

Which Certifications to Pursue

Certifications can help get your foot in the door when seeking cybersecurity employment. The problem is there are so many of them, and it's hard for aspiring cybersecurity professionals to decide which to pursue. But ISC2 is making the journey easier for newcomers. ISC2 created a certification for entry- and junior-level cybersecurity professionals called ISC2 Certified in Cybersecurity. This foundational cybersecurity certification creates a pathway to a rewarding career in cybersecurity for many around the world. Anyone earning the ISC2 Certified in Cybersecurity certification demonstrates they have the foundational knowledge, skills and abilities to take on entry- and junior-level cybersecurity roles, enabling employers to more confidently build resilient teams across all experience levels.

The ISC2 Certified in Cybersecurity certification exam evaluates candidates across the following subject areas:

- Security Principles
- Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts
- Access Controls Concepts
- Network Security
- Security Operations

More details about the exam subject matter are available through the ISC2 Certified in Cybersecurity exam outline.

Free Cybersecurity Certification
ISC2 has pledged to expand and diversify the cybersecurity workforce by providing free ISC2 Certified in Cybersecurity education and exams to one million people worldwide. To qualify, individuals must enroll as an ISC2 Candidate, for free, which entitles them to a wide array of exclusive programs and services to assist individuals starting a cybersecurity career, including free education and exams.

Anyone seeking employment in cybersecurity will discover a vexing paradox – professionals are badly needed but it's a challenging industry to get into. Employers tend to have unrealistic expectations about candidates for the jobs they want to fill. As a pursuer, this means you have to work hard to land a job.

Here are five main takeaways to keep in mind in strategizing your job pursuit:

Do Your Homework

You must put in time to learn about the industry and its diversity of roles and keep up with developments in a very dynamic field.

Emphasize Transferrable Skills

Figure out how to put your background and skills to use as a cybersecurity professional so you can attract the attention of hiring managers and ultimately succeed in the field.

Focus Your Pursuit

Recognize that no single cybersecurity professional can fulfill all roles in the cybersecurity field, so pick a track to pursue based on your skills and experience.

Be Persistent

You may have to break through hard-to-overcome, preconceived notions by employers about what a qualified candidate for a cybersecurity position has to offer.

Show Your Passion

Approach your pursuit with passion, and you will boost your chances of getting hired because a prospective employer will see your dedication.

Cybersecurity offers rewarding careers. With so many different tracks to follow, it can lead you down unexpected and gratifying paths. To succeed, you must work hard and always be

learning. And if you succeed, your rewards are job stability and security and ample opportunities to grow in a dynamic field.

Note: If you have any suggestions or are interested in joining the conversation. Please reach out to us at community.isc2.org or send an email to communications@isc2.org.