ISC2

Is a Career in Cybersecurity RIGHT FOR ME?

- Th

Inside

Why Cybersecurity?

With the current threats to cyber stability around the world, there's never been a greater urgency for cybersecurity professionals than now. 2021 recorded the largest annual increase in cyberattacks in six years. And the outlook is worsening. Organizations say it's almost certain — 76% likely — they'll be compromised by a cyberattack in the next 12 months.[1]

Around the world, organizations are investing an increasing amount of time, money and talent to detecting and mitigating cyberattacks. The result is a boom in demand for skilled cybersecurity professionals.

Whether you're just starting out in your professional career or looking to do something new, here are four reasons to consider joining the exciting and rewarding field of cybersecurity.

1. Work where life lands you with near limitless employment potential. Whether you feel the itch to travel and experience different cultures or want to stick closer to home, cybersecurity will take you there. The demand opens near limitless opportunities for skilled professionals around the globe.

2. Choose any industry that intrigues you. Every industry needs skilled cybersecurity professionals to protect their networks, data

[1] Cyberthreat Defense Report

and online transactions. It's not just government agencies, healthcare and financial institutions dealing with bad actors, even sectors that haven't traditionally focused resources on cybersecurity now find themselves under threat.

3. Work in the area of cybersecurity that interests you most. There are many different career pathways in cybersecurity. This dynamic, rapidly evolving field offers the opportunity to model your career to match your interests. The National Initiative for Cybersecurity Careers and Studies identifies 52 distinct cybersecurity roles; the right one for you is out there.[2]

4. Find job security in a field that's future-proof. Cybersecurity is expected to see continued extensive job growth for the foreseeable future. By 2025, 3.5 million job openings are expected in the field.[3] And with technological advances showing no sign of slowing, the need will continue into the foreseeable future.

[2] National Initiative for Cybersecurity Careers and Studies, Cyber Career Pathways Tool
[3] Cybersecurity Ventures, Cybersecurity Jobs Report

Cybersecurity Needs You:

Help Close the Workforce Gap

Everyone everywhere needs more cybersecurity professionals for a safe and secure cyber world. Now is a prime opportunity for you to enter this exciting and rewarding field.

The ISC2 Cybersecurity Workforce Study collected survey data from more than 4,700 cybersecurity professionals working with small, medium and large organizations throughout North America, Europe, Latin America and Asia-Pacific. The findings shed light on how the lingering effects of the pandemic and the accelerated evolution of the threat landscape impact organizations' security practices and the role cybersecurity professionals play in defending our critical assets.

The study provides two critical measures of the cybersecurity profession — the Cybersecurity Workforce Estimate and the Cybersecurity Workforce Gap.

The Cybersecurity Workforce Estimate presents an appraisal of the available pool of cybersecurity professionals worldwide. The study estimated there are 4.19 million cybersecurity professionals worldwide.

By contrast, the Cybersecurity Workforce Gap is the number of additional professionals organizations need to adequately defend their critical assets. The global cybersecurity workforce needs to grow 65% to effectively defend organizations' critical assets. That requires a massive influx of 2.7 million professionals to meet demand.

Do a search for cybersecurity jobs at LinkedIn, and you'll get hundreds of thousands of results — and that's just in the United States. Even as more than a million people in the U.S. currently work in cybersecurity, there are more than 700,000 unfilled positions.[4]

Now let's look at some of the specific roles both at entry-level and further along the cybersecurity career pathway.

[4] CyberSeek, "Hack the Gap" online tools and data

Consider These Careers in Cybersecurity

As you consider a career in cybersecurity, you'll find it's not a homogeneous field limited to a handful of roles. Rather, cybersecurity covers a variety of functions and responsibilities, and is reliant on teams with diverse skills, experiences and ideas.

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 help you narrow the field for the roles that may interest you the most.

Entry-Level Cybersecurity Job Roles

Security Analysts examine information to help identify risks and threats, then recommend and help implement strategies to stop those threats from damaging the organization's network or property. In this role, analysts typically work under a senior analyst to develop skills and learn more about the tools and techniques required to be more effective on the job.

Security Specialists have responsibilities essential to the security of an organization's information systems. Duties include identifying potential security issues using a mix of knowledge and special programs; setting security standards; educating management on best technologies and security practices; upgrading information security software; and assisting with security incidents.

Security Architects design security environments and systems to defend against malware and other intrusions to computer systems. Once structures and systems are in place, they run an audit to test for weaknesses or vulnerabilities. They plan, research and design security architecture and perform vulnerability testing and security assessments of software and systems.

Security Auditors are responsible for verifying an organization's security procedures against a framework. The goal is to ensure a system's strength and report vulnerabilities encountered while examining the system. They locate flaws within information systems, evaluate the security of IT systems and utilize the organization's processes and practices to ensure audits are completed correctly.

Forensic Specialists/Analysts examine and recover data from computer systems. The information may then be used as

evidence in both criminal and civil cases. They recover lost or encrypted data and investigate data trails. They analyze this information and prepare recovered data for use as evidence in court.

Junior Penetration Testers improve computer network and systems security by attempting to find and exploit vulnerabilities that threats could use against clients. They plan and execute evaluation tests, stay informed about current cybersecurity threats and program software to aid penetration tests.

Security Engineers handle digital security for organizations. They provide input for security protocols, operate cybersecurity systems and maintain IT security infrastructure. They are responsible for testing and screening security software and monitoring networks and systems for security breaches or intrusions.

IT Auditors are responsible for evaluating the application of an organization's IT systems or databases against a framework. Their duties include setting audit objectives; gathering data by interviewing department employees or comparing current procedures to IT department standards; and creating actionable plans to improve IT systems.

Systems Administrators oversee the maintenance and security of information systems. Their duties include installing antivirus or malware protection software, responding to employee concerns, drafting internal documents to help employees use computer systems and coordinating with leadership to determine new technologies that enhance the organization's information systems.

Aspirational Cybersecurity Job Roles

Cybersecurity professionals in entry-level roles often pursue advance certifications and progress to roles with more career opportunities and responsibilities, including:

- Chief Information Officer (CIO)
- Chief Information Security Officer (CISO)
- Director of Security
- Enterprise Architect
- IT Director/Manager
- Network Architect
- Security Administrator
- Security Analyst
- Security or Systems Architect
- Security Auditor
- Security Consultant
- Security and/or Systems Engineer
- Security Manager

The Essential Skills You Need

How can you know if cybersecurity is right for you? Roles at all levels require this core set of essential skills.

Leadership and communication. You should demonstrate credibility, responsiveness and ethics. Strong communication skills can help you earn trust from senior management and your peers.

Passion for learning. You'll be expected to continuously learn the latest cybersecurity trends, technologies and security challenges facing organizations. You must be passionate about learning and professional growth to be successful.

Determination. You must be persistent in the ever-changing threat landscape. You'll be expected to see a solution through to completion and never stop until the challenge is solved.

Collaboration. Cybersecurity is a shared responsibility across the organization. Professionals must be collaborative and work at all levels to instill a culture that ensures security policies are not only in place but followed. It is also critical to gain buy-in throughout the organization for security initiatives.

Analytical and critical thinking. You'll be expected to be analytical regarding how incidents occur, the attack surfaces prone to exploitation and how to minimize cyber-attacks. An analytical and insightful security professional anticipates how hackers will exploit the network and its applications.

How to Get Your Foot in the Door

What's the best way to break into cybersecurity? It depends where you are in your career, what you want to do and where you see your future. If you thrive on solving problems, are driven to help people and are stoked at the prospect of working in a constantly evolving field, you already have a lot in common with today's cybersecurity workforce.

You don't need an IT degree to work in cybersecurity. In fact, more than half of cybersecurity professionals got their start outside of IT, transitioning from unrelated careers, getting their start with cybersecurity education and exploring cybersecurity concepts on their own.

Here are some fundamentals to consider, whether you're a student or a professional.

Advice for Students

Know the technical basics. Not everyone in cybersecurity comes from a deep technical background, but it's important to know the basics. Some industry experts

advise starting on a more general technical path and then focusing on security later, once the basics are mastered. Whatever path you choose, you will need a general understanding of systems, coding, networking, and how applications are run and maintained.

Get certified. Certifications can help you get your foot in the door. Working professionals say they're the most important way for career pursuers to enter the field.[5]

Consider training in general IT. Finding an internship, apprenticeship or entry-level job in IT is a great launch pad. Consider data entry, help desk or any other ground-level technical position to learn IT fundamentals. You'll get a hands-on sense of technical processes and real-world business scenarios that will serve you well in cybersecurity.

Focus your area of interest. What does your ideal cybersecurity career look like? Your path in the short term will springboard your future. Roles that pave the way include systems administrator, web administrator, web developer, network administrator, IT technician, network engineer and software engineer.

Learn independently. There are many ways to learn the technical skills used in cybersecurity, including books, self-directed learning (teaching yourself how to code, for example), online courses and guided training. Whichever you choose, these fundamentals will be essential as you get deeper into security work.

[5] Cybersecurity Career Pursuers Study

Advice for Professionals

For incoming professionals just starting in cybersecurity, persistence is key. Don't give up if your first few attempts to get in front of a hiring manager fall flat. Keep in mind, many recruiters are focused on processing applications and candidates across an entire organization. Your goal is to reach the hiring manager. Here are some ways to connect with people in the field to get there.[6]

- **Online Communities** - There are many active forums on social media, including Reddit, LinkedIn and more, where you can connect, research your questions and learn from other cybersecurity professionals' experiences and opinions.
- **Cybersecurity Chapters** - Local chapters around the world focus on creating in-person and online networking opportunities for cybersecurity professionals. Many first-timers find professionals who are willing and eager to share their experiences and advice.
- **Industry Events** - Cybersecurity conferences provide networking opportunities to get in front of the right people, including recruiters, hiring managers and cybersecurity team members who can help open doors into their organizations.

Incoming professionals should also absorb as much information as possible about the roles and responsibilities associated with the job titles that intrigue them most. That way, once you get in front of a recruiter or hiring manager, you're ready to:

- Ask questions and share opinions that demonstrate knowledge of the profession, as well as the current threat landscape.
- Emphasize an understanding of the skills required 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.

[6] How to Get a Cybersecurity Job

How Certification Factors In

Cybersecurity professionals say the most important way to enter the field successfully is through certification.[7] They point to certification as an achievement and a proof point to their employers, peers and themselves that validates their skills.

Certified in Cybersecurity from ISC2 — the new entry-level certification from world's leading cybersecurity professional organization known for the CISSP® — gives you the knowledge and skills you need to begin your first role ready for what's next.

No Experience Required

No work experience in cybersecurity or formal educational diploma/degree is required to take the exam. If you're a problem-solver with an analytical mindset, Certified in Cybersecurity (CC) is right for you.

When you successfully complete the exam, you'll gain immediate access to valuable ISC2 membership benefits, including thought leadership, exclusive networking and more.

[7] Cybersecurity Career Pursuers Study

More Benefits of Certification

- Respect - Validate your knowledge and build credibility.
- Job offer and advancement - Gain the solid foundation of cybersecurity knowledge employers are looking for, from an association they trust.
- Growth and learning - Develop new skills you can apply in day-to-day work.
- Pathway to cybersecurity careers and advanced certifications - Build a strong foundation for an infosec career and become familiar with exam formats for advanced ISC2 certifications like CISSP.
- Community of professionals - Access a network of peers and CPE/learning opportunities.
- Higher salaries - ISC2 members report 35% higher salaries than non-members.

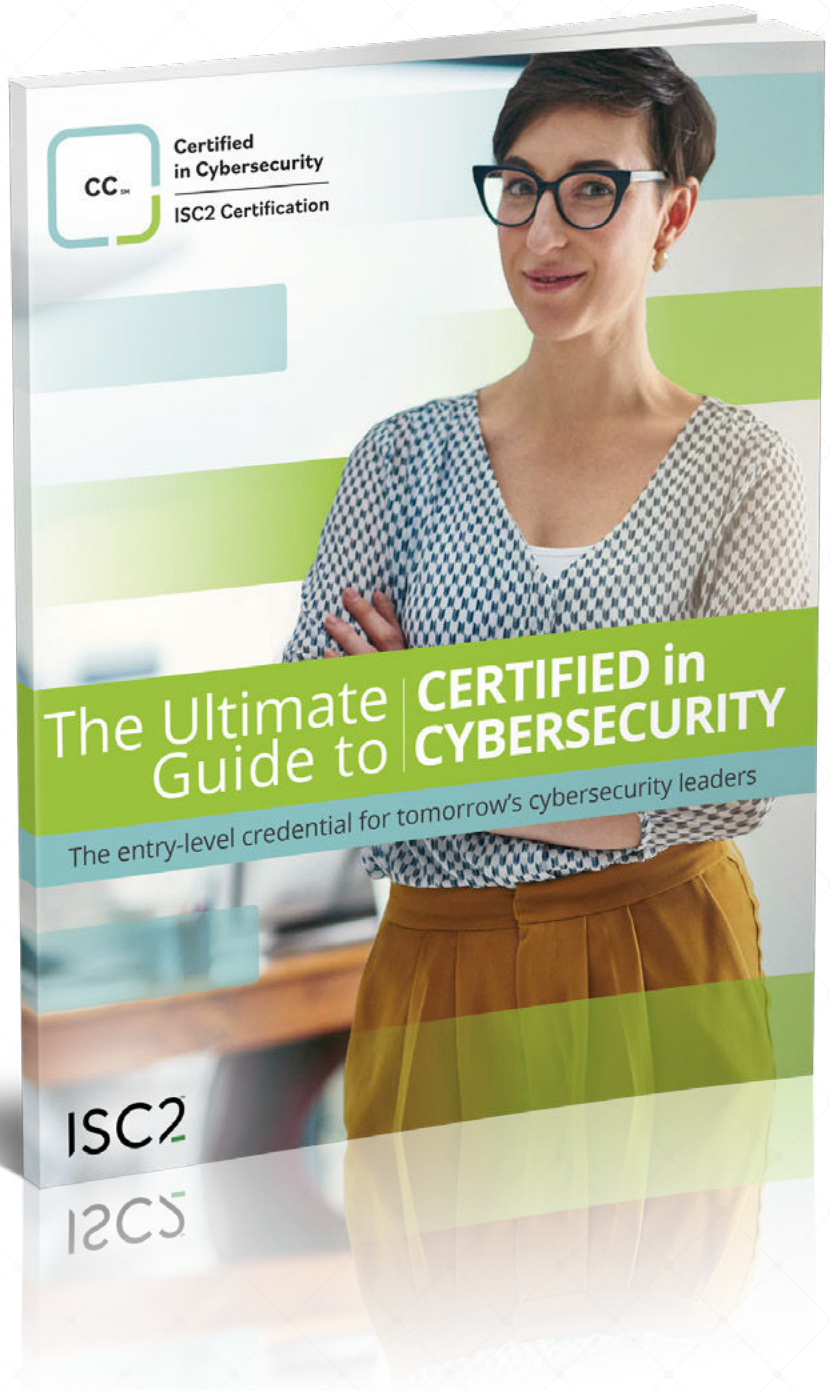
Next Step: The Ultimate Guide to Certified in Cybersecurity

Take the next step toward a career in cybersecurity with The Ultimate Guide to Certified in Cybersecurity: The Entry-Level Credential for Tomorrow's Cybersecurity Leaders. It covers everything you need to know about the credential. Find out how Certified in Cybersecurity and ISC2 can help you discover your certification path, create your plan and acquire the knowledge and skills for a successful career in cybersecurity.

Inside: Your Questions Answered!

- What's Covered in the Exam?
- What are the Exam Prep Options?
- What are the Benefits of Certification?
- Plus, Real-World Testimonials

Get Your Guide



From the World's Leading Cybersecurity Professional Organization

ISC2 cybersecurity certifications, including CISSP and CCSP, are recognized globally as the gold standards for excellence.

Elite Cybersecurity Professionals

ISC2 members represent an elite global network of information security professionals. They are top experts in their fields, dedicated to the highest ethical standards and best practices. Our members work for governments and highly respected companies around the world. Through ISC2 certifications, they show superior competency.

Members Around the World

ISC2 is the world's leading cybersecurity professional organization, nearly 500,000 members strong. Our members work in high-level cybersecurity, information, software and infrastructure positions all around world.

Far-Reaching Impact

The professionals who make up the ISC2 community play a vital role. They not only protect the organizations they serve, they help keep society safe and secure. And they're in high demand, as organizations place more importance on information security.