ISC2

# Step Into Cybersecurity

## How to Navigate Your Path into the Profession

# Inside

# Balancing Opportunity and Demand

Driven in part by the rapid expansion of cloud and AI technologies and the increased pace of cyberthreats, the need for skilled cybersecurity professionals has never been greater. The World Economic Forum reports only 14% of global organizations have the necessary skilled talent to meet their cybersecurity objectives, and two-thirds of organizations remain vulnerable to cyberattacks and breaches due to a lack of critical skills.[1]

With the current threats to cyber stability around the world, there's never been a greater urgency for skilled cybersecurity professionals than now. Nearly nine in 10 (88%) professionals surveyed for the Cybersecurity Workforce Study have experienced at least one significant cybersecurity consequence in their organizations because of a skills shortage, and 69% have experienced more than one.[2]

However, the job market for new entrants is complex. Economic and geopolitical factors, in addition to reduced corporate budgets, have challenged hiring managers charged with recruiting and retaining staff with the skills for critical roles.[3] On one hand, many job openings have been left unfilled. On the other hand, the current hiring environment has put both entry-level and senior cyber professionals in the spotlight. New entrants to the industry will need to be called upon to fill essential roles in the long term.

By understanding the different focus areas within cybersecurity, mastering the technical and soft skills, making industry connections and earning the right certifications, candidates can secure a vital foothold in this highly valued and rewarding profession. In this white paper, we will explore:

- Today's cybersecurity employment landscape
- Pathways into the profession
- Entry-level roles and expectations
- Practical tips for navigating the job market
- The value of ISC2 certification

# Cybersecurity Job Market Outlook

Alongside the headlines earned by AI and big data, networks and cyber skills rank as the second fastest-growing skill category globally.[5]

However, the hiring market is not uniform in its demand at all skill levels:

## Entry-Level Candidates

Many job postings for junior or analyst roles list prerequisites such as one to three years of experience or cyber certifications.

## Mid-Level Career Transitioners

These individuals typically bring five to ten years of professional experience, often in adjacent fields where skills can be leveraged into specialized cybersecurity domains.

## Upper-Level Career Transitioners

These professionals often have management experience and target strategic roles focused on risk, governance and business alignment.

# How Do Hiring Managers Plan to Fill Critical Roles?

Cybersecurity hiring trends research reveals:

- **Security managers prioritize hands-on experience and certifications over relevant education.** Most would consider candidates with only previous IT work experience (90%), or those who only hold an entry-level cybersecurity certification (89%), over those with only education in IT, cybersecurity or computer science. For these managers, relevant experience and certifications can outweigh a degree alone.[3]
- **About a quarter of cyber hiring managers that recruit from education programs have identified entry- and junior-level cybersecurity talent from programs outside of computer science, IT or cybersecurity,** highlighting an opportunity to bring fresh perspectives to the field by broadening the talent pool.[3]
- **Cybersecurity hiring managers value nontechnical skills as much as, or in some cases more than, technical skills.** Teamwork, problem-solving and analytical thinking rank highest, ahead of data security and cloud security. This signals that hiring managers are looking for more than technical know-how — they seek collaborative, adaptable thinkers who can tackle the complex problems impacting the cybersecurity landscape.

Entry-level roles frequently take little time to fill. Close to a quarter (21%) of hiring managers say these roles are typically occupied in under a month, with another 40% reporting it typically takes one to three months. For junior-level roles, 8% say these positions can be filled in less than a month and 34% within one to three months. Senior roles often require longer timelines to fill.[3]

# Pathways Into the Profession

Professional paths into cybersecurity are no longer a linear progression defined solely by a four-year degree. The industry has increasingly adopted a skills-first approach, recognizing that practical ability and validated knowledge can be acquired through a range of approaches.

Common pathways into the field include:

## No Degree

Many candidates have completed some college coursework in areas like computer science, mathematics or business but may not hold a bachelor's degree. This academic background, when combined with focused training, can be a compelling entry point, with the focus shifting toward certifications, practical experience and networking.

Internships and apprenticeship programs are helpful for early cybersecurity careers. Typically, internships are short-term placements (often during or after college). Apprenticeships are longer term and combine on-the-job training with formal instruction and often lead to job offers upon successful completion. Internships (55%) and apprenticeships (46%) are considered effective tools for identifying and recruiting early-career cybersecurity talent.[3]

## University Degrees

A formal university degree in cybersecurity, computer science, information technology or engineering remains a strong pathway, particularly for large enterprises, government work and entry into specialized fields like research or forensics. A master's degree is often useful for mid-career professionals looking to solidify their expertise.

## Certifications and Certificates

Cybersecurity certifications and certificates are key differentiators for candidates without traditional degrees. This path focuses on demonstrating verified skills and specific domain knowledge. Entry-level certification can signal a candidate's dedication to building their skill set, starting with foundational knowledge. Certificates often involve completing a course or training curriculum and enable rapid skill acquisition and portfolio building, but they are generally viewed as less rigorous than certifications.

## Career Transitions

Strategically mapping existing skills to cybersecurity domains may meet entry-level requirements. For example, a project manager's skill set may translate well into security program management, and IT professionals may leverage their technical expertise in networking or operating systems for roles like SOC analyst or security engineer.

At every career level, but especially those looking to enter the field with minimal experience, heeding the following advice can yield competitive advantages:

- Know the technical basics. For those without deep tech backgrounds, try starting on a more general path and mastering the basics prior to focusing on cybersecurity.
- Pursue IT training. Develop experience in technical processes and real-world business scenarios through entry-level technical positions, such as data entry or help desk, to learn IT fundamentals.
- Focus on areas of interest. Choose an industry that captures your attention. Every sector faces cyberthreats. Work in cybersecurity areas of focus, such as cloud or network security, that match your interests.

It's also crucial to consider what factors are driving the pursuit of careers in cybersecurity. According to an ISC2-commissioned study, top motivators for professionals include:[6]

- The ability to solve problems (52%)
- The environment with its high demand for technical and nontechnical skills (44%)
- The ability to help people and society as a whole (37%)

# Entry-Level Roles and Expectations

Cybersecurity managers have a responsibility to defend their organizations against cyberthreats. Entry-level candidates can help maximize their likelihood of meeting these expectations by achieving a healthy balance of technical execution and critical nontechnical skills.

## Technical Skills

Entry-level candidates should be proficient in the underlying technology that security measures defend. Be prepared to demonstrate your knowledge in action. Most organizations (84%) use skills-based assessments and/or tests for entry- and junior-level cybersecurity applicants.[3]

Core technical skills cover:

**Networking Fundamentals** These include a deep understanding of the TCP/IP model, network protocols, routing, switching and common network services (DNS, DHCP).

**Operating Systems (OS) Administration** This includes competence in both Windows and Linux environments, such as command-line interfaces (CLI).

**Security Tools and Concepts** Knowledge of fundamental security concepts like encryption, hashing and the principle of least privilege is mandatory, as well as hands-on experience with security information and event management (SIEM) systems, intrusion detection systems and firewalls.

**Cloud Fundamentals** Given that cloud security is one of the highest-demand areas of focus, knowledge of cloud computing platforms (e.g., AWS or Azure) is key.

# Nontechnical Skills

Critical thinkers and team players exhibit these six skills sought by hiring managers:

### 1. Problem-Solving

Effective team members must work out how attackers are able to gain access to a system, even when they have no prior knowledge of the methods used by bad actors.

### 2. Analytical Thinking

Cyber professionals need to anticipate how hackers will exploit the network and its applications and how to mitigate attacks. They must think like an attacker and identify the vulnerabilities ahead of time.

### 3. Critical Thinking

The challenges of working in this rapidly changing and complex field requires analyzing problems and evaluating alternatives, as well as the ability to clearly explain what needs to be done and why.

Critical thinking enables cybersecurity professionals to:

- Make high-stakes decisions about data security
- Assess and manage technology risks
- Plan, evaluate and implement cybersecurity measures
- Respond to security breaches or threats
- Explain threats, options, plans and progress to senior leadership and coworkers

### 4. Ability to Work Independently

Candidates must be able to work on their own to get the job done. Since this effort is often individual in nature, taking initiative and being a self-starter are key.

### 5. Teamwork

Cybersecurity teams that perform at the highest levels are comprised of members who effectively collaborate and work toward accomplishing shared goals. These individuals must be able to anticipate, coordinate and ultimately achieve efficient workflows.

### 6. Creativity

Bad actors don't play by the rules. Cybersecurity teams must think creatively about preemptive threat protection and, in the case of an attack, rapid response and mitigation.

# Strategies to Stand Out

Entry-level cybersecurity candidates can take definitive steps to improve their visibility, build a credible professional profile and overcome hiring hurdles at any level.

### 1. Identify Your Area of Focus

Cybersecurity covers a variety of functions and responsibilities. Determining where your interests and skills lie will help shape your career journey.


Cloud Security | Cybersecurity Leadership | Entry-level Cybersecurity | Governance, Risk and Compliance | Network Security | Security Operations | Software Security

### 2. Work with Mentors

Cybersecurity professionals say that having a mentor to shadow in their first three years in the field was invaluable for their success.[7] What's more, mentorshipgives senior team members a chance to demonstrate leadership and take on more responsibility.

### 3. Connect with Networks

Networking is indispensable for gaining insights from established professionals and finding opportunities that may not be well advertised. The first step is finding local groups, such as ISC2 chapters, and attending industry events.

- Attend meetings and events on a regular basis to build familiarity and trust.
- Volunteering can be the most efficient way to meet the most connected people in the chapter.
- Offer value to fellow cyber professionals. This could be sharing relevant news articles or introducing two people who should know each other. Helping others often has a way of helping you.
- Ask for advice, not jobs. Positions may not be immediately available but curiosity about building skills can open the door for mentorship and referrals.

- At events, have an elevator pitch ready by practicing a concise answer to "What do you do?" and focusing on your target role.
- Target event sponsors who attend events with the intent to hire.
- Track your connections, including where you met and what you discussed. This helps facilitate future follow-ups.

### 4. Leverage LinkedIn

Research shows that a candidate's online presence matters. More than half of hiring managers (54%) say they have passed on candidates due to their social media activity.[3] However, it's best to think of platforms like LinkedIn less like a risk and more like an opportunity.

LinkedIn can help candidates further their networking and build meaningful connections. Sending personalized connect requests to recruiters and hiring managers, joining relevant cybersecurity groups and posting content consistently can highlight your commitment to the field.

What's more, once people visit your LinkedIn profile, make sure it's optimized with the right keywords and an engaging summary that tells your professional story, highlights your passion for security and quantifies your achievements.

### 5. Join an Online Community

Engaging with a likeminded group of aspiring and working cybersecurity professionals can provide answers and encouragement in the job hunt. For example, the ISC2 Community is an online forum for discussion on cybersecurity topics, certification support and job postings, where members and non-members can ask questions and share knowledge.

# Value of ISC2 Certification and Membership

When hiring managers are asked about the most critical attributes to a candidate's prospects, certifications come out on top: IT/cybersecurity certifications (47%) ranked slightly higher than IT experience (44%) and relevant education (43%).[3]

ISC2 Certified in Cybersecurity (CC) certification demonstrates to employers that candidates have the key foundational concepts in information security, determined by experts and practitioners working in the field.

CC certification serves a range of people making the transition to different positions within the industry. Some 45% of CC holders reported already working in cybersecurity. Of those who worked in cybersecurity prior to getting certified, the median work experience was six years. For those working in IT – but not cyber – before getting certified, the median work experience was 10 years.[7]

The first step is applying to become an ISC2 Candidate, which opens opportunities to build connections with a global membership of leading minds that can open doors. ISC2 Candidates also gain access to a wide range of benefits and support along the way, including access to Official ISC2 CC Online Self-Paced Training and a CC exam voucher. CC starts newcomers on their path to advanced certifications like the CISSP, cybersecurity's gold standard credential for future leadership roles.

As an ISC2 member, you'll stand at the forefront of tackling cybersecurity challenges, equipped with the knowledge and skills sought by employers. You're an integral part of the world's leading member organization for cybersecurity professionals, representing certified professionals around the globe.

Regardless of where you are in your cybersecurity career journey, ISC2 is there for you every step of the way. Its best-in-class professional development programs, training, certificates, exclusive benefits and more will help you distinguish yourself from your peers, stay relevant and maintain your crucial certifications.

Get your strongest start in cybersecurity.

**Sign up to become an ISC2 Candidate — your first year is free.**

04/2026

## References


1. Global Cybersecurity Outlook. *World Economic Forum.*
2. Cybersecurity Workforce Study. *ISC2.*
3. Cybersecurity Hiring Trends. *ISC2.*
4. Cybersecurity Supply/Demand Heat Map. *CyberSeek.*
5. Future of Jobs Report. *World Economic Forum.*
6. 6 Essential Skills to Hire for in Cybersecurity. *ISC2*.
7. Who Earns the ISC2 Certified in Cybersecurity Certification? *ISC2.*