EMPLOYMENT

SPONSORED BY eSENTIRE

2023 Official Cybersecurity Jobs Report

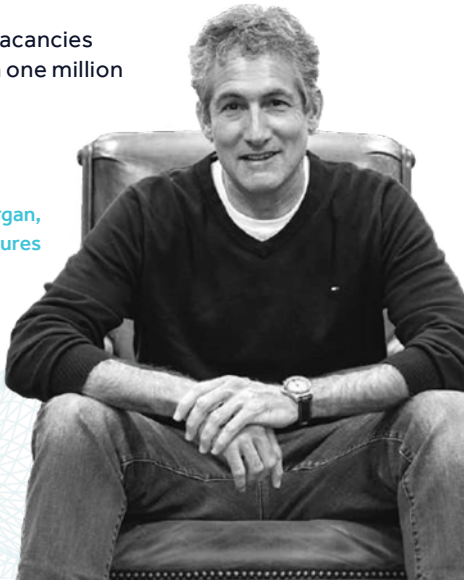
3.5 million unfilled cybersecurity jobs to remain through 2025.

CYBERSECURITY VENTURES

Introduction

Global cybersecurity job vacancies grew by 350 percent, from one million open positions in 2013 to 3.5 million in 2021.

Steve Morgan,
founder of Cybersecurity Ventures



The number of open positions leveled off in 2022, and remains at 3.5 million in 2023. Industry efforts to source new talent and tackle burnout continues, but we predict that the disparity between demand and supply will remain through at least 2025.

– ***Steve Morgan**, founder of Cybersecurity Ventures and Editor-in-Chief at Cybercrime Magazine*

Table of Contents

Talent Crunch

Last year, Microsoft pledged to help fill the 3.5 million open cybersecurity vacancies expected globally in 2025, as predicted by Cybersecurity Ventures.

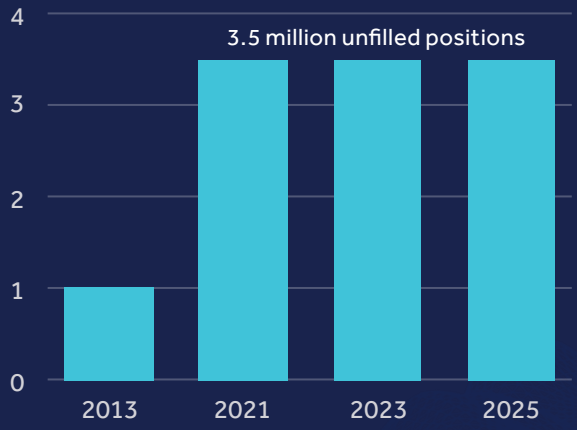
The Redmond giant's promise to expand a national skilling campaign in the U.S. to 23 additional countries represents an industry-wide effort to increase the available talent pool.

With enough unfilled cybersecurity jobs in 2023 to fill 50 NFL stadiums, a growth of **350 percent** over a decade, we expect the shortfall to hold fast until industry leaders and educational institutions provide more incentives, training opportunities, and remove barriers to entry.

Organizations of every size and type have faced a tumultuous few years due to the pandemic and economic uncertainty. These challenges have likely impacted recruitment, and may continue to do so.

Talent Crunch

The number of unfilled cybersecurity jobs globally has leveled off since 2021. (Figures below are in millions)



Talent Crunch

A recession on the horizon could cause further woes – but may also represent an opportunity for new career seekers.

Since **1945**, the U.S. has experienced 13 recessions. While many economists do not believe the U.S. is yet amidst another one, it is a possibility considering global warfare, supply chain disruption, and surging inflation.

Recessions tend to wipe out millions of jobs. For example, the 2008 recession resulted in Americans losing an estimated 2.6 million jobs, with the loss of roles generally concentrated to industries vulnerable to poor economic outlooks.

Some industries fare better than others, such as healthcare or law enforcement – necessary in or outside a stagnant economy. As jobs are lost, other markets expand and may present opportunities to upskill and take the first steps to a new career path.

While tech firms are firing, the cybersecurity segment is hiring, according to a recent FOX Business story. Technology firms have shed more than **300,000 jobs in the past two years** with more on the way.

While Amazon, Meta, Twitter, Microsoft, Google, and the other tech giants are going through layoffs, our industry has hung out an enormous **Help Wanted** sign. We expect brisk hiring in the cybersecurity space for the rest of this year, and through 2025.

Steve Morgan, Founder of Cybersecurity Ventures

Cybersecurity is a prime market to enter. As so many job roles are unfulfilled, private organizations, governments, and higher education alike are exploring new avenues to recruit and train talent, including early career programs. In the **U.S.** alone, there are around 750,000 unfilled cybersecurity jobs as of Apr. 2023. For anyone seeking to retrain, the time is now.

Technology Workforce

There was a surge of hiring by countless technology companies following COVID-19.

Despite initial enthusiasm in the IT space, the situation changed in early **2023**. As a result, many enterprise companies laid off high percentages of their workforce. Meta, Twitter, IBM, Alphabet, GitHub, Microsoft, and Yahoo are among those that have made tens of thousands of IT workers redundant between them.

According to redundancy tracker Layoffs.fyi, which has been tracking layoffs since the pandemic, 470 technology firms have reduced their workforces, as of Mar. 2023.

Hiring sprees, then subsequent revenue declines, created a perfect storm of mass layoffs. Although, for some organizations, the cuts could be akin to backtracking to pre-COVID staffing levels.

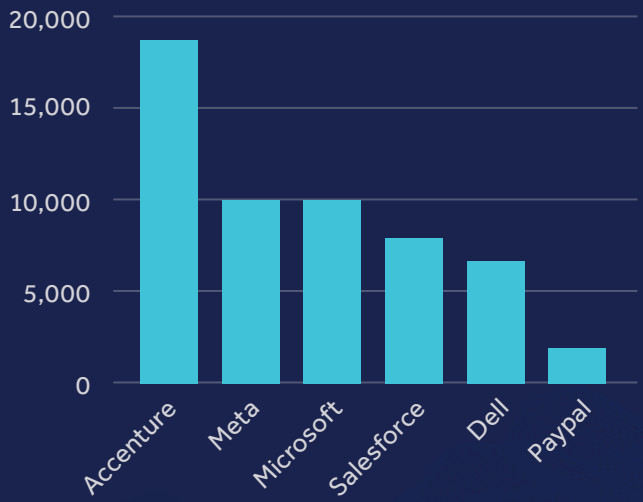
Despite the disarray of the tech industry, cybersecurity remains a near-zero unemployment marketplace for those with extensive backgrounds, and the shortage means that IT teams must also shoulder a security burden. Staff must train in modern threat awareness, including phishing, social engineering, Business Email Compromise (BEC), and financial fraud. They must also know how to protect and defend apps, data, devices, infrastructure, and people.

The unemployment rate for tech occupations is still low at **2.2 percent**, which indicates tech employees are being reabsorbed back into the workforce, Tim Herbert, chief research officer with the tech trade association CompTIA, told The Wall Street Journal.

Technical services and software development, a subsector made up of mostly small and midsize firms, added the most tech workers in the past year, so workers seem to be **transitioning from big tech** companies to startups, cybersecurity and technical consulting firms, Herbert said.

Technology Workforce

Recent tech layoffs reported by TechCrunch:



Cybersecurity Workforce

The IT industry was growing before the pandemic. A silver lining of mass redundancies is a talent pool of recently unemployed workers with desired, transferable skills that would make them exceptional in cybersecurity roles.

According to the **U.S. Bureau of Labor Statistics**, the average growth rate for all occupations in the U.S. between 2021 and 2031 is an estimated 5 percent. However, the projected job outlook for "Information Security Analysts" is 35 percent – a growth far beyond the average.

There is a **strong demand** for IT services including cybersecurity and cloud computing, of which entry- level and mid-level roles only sometimes require qualifications.

There is also a need for more candidates with gold- standard cybersecurity certifications in the U.S.

The global cybersecurity workforce consists of around 4.5 million people in 2023.

There are just over 94,000 **CISSPs** (Certified Information Systems Security Professionals) nationwide, according to CyberSeek, but more than 134,000 job openings require CISSP certification. A security analyst can earn up to **25 percent more** with a CISSP Certification.

It's also important to understand that the CISSP designation is not an entry-level certification." says Greg Crowley, CISSP, CISM, and CISO at eSentire. "It requires the certificate holder to have a minimum of five years verified work experience in cybersecurity. If you pass the exam without meeting the experience requirements you are not actually a CISSP. This means either companies don't understand what they are asking for or they have set the bar too high for entry-level positions.

Greg Crowley, CISSP, CISM, and CISO at **eSentire**

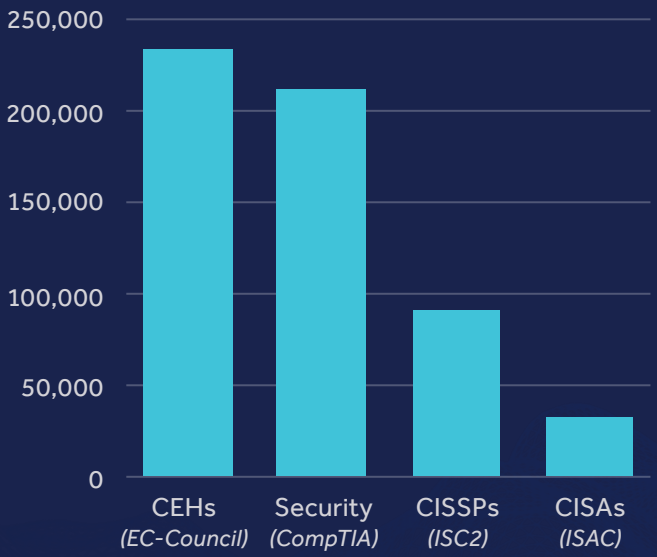
Or consider CISAs (Certified Information Systems Auditors), with just over 37,000 people holding the credentials but over 87,500 advertised jobs requesting them.

However, there's a robust pool of entry-level candidates, with 213,000 holders of CompTIA Security+, and only 101,000 openings requiring it.

More than 237,000 people have been awarded CEH (Certified Ethical Hacker) status by EC-Council, the fourth most desired among cybersecurity jobs.

Cybersecurity Workforce

Number of people with desirable certifications:



Cybersecurity Salaries

The U.S. Bureau of Labor Statistics **estimated** that the median salary for an "Information Security Analyst" was $102,600 in 2021. Compensation in 2023 ranges from **$82,000** to **$107,000**, on average, for cybersecurity analysts in the U.S. The most experienced employees have reported salaries of over $142,000, according to online aggregators.

Glassdoor **data** suggests the average pay of a CISO (Chief Information Security Officer) in 2023 is $182,000, rising to $300,000 in the highest tiers. In a handful of U.S. cities, CISO salaries have ranged from **$350,000 to $420,000** going as far back as 2016.

Private organizations are investing heavily in cybersecurity recruitment. Consulting giant Booz Allen pays its entry-level cybersecurity employees between $95,000 and $150,000, which can reportedly reach up to $240,000 with experience.

Graduates with Master's degrees **report an** average pay of $214,000.

Big Tech

We have observed the stirring of competition by enterprise organizations looking to secure and train the next generation of cybersecurity defenders and leaders.

Businesses are also creating new avenues for entry as alternatives for degree-level studies to develop and retain talent pipelines.

Advanced degrees and certifications, including CISSP, are well-respected but are not the only paths to a lucrative cybersecurity career. Many organizations are pivoting to internships, scholarships, college recruitment, and internal retraining programs.

For example, Microsoft is expanding a major training initiative from the U.S. to 23 countries.

Google has committed **$10 billion** to advancing cybersecurity and has pledged, via the Google Career Certificate program, to train 100,000 Americans in roles ranging from data analytics to cybersecurity.

In 2022, SANS, Google Cloud and Palo Alto Networks **partnered** with Cyversity to launch the Global Cyber Diversity Academy, a program designed to close the "great cyber divide" for talented candidates wanting to enter cybersecurity.

HPE **runs** the Global Security Early Career Program and an internship scheme to recruit college attendees to work while they study and gain experience in corporate security.

IBM planned to **train** 150,000 people in cybersecurity skills between 2021 and 2023. The company also operates IBM SkillsBuild, a free STEM learning program made possible with 45 collaborations worldwide to offer IT career study pathways, including cybersecurity.

Higher Ed

Research from Cybersecurity Ventures has been vetted and cited by colleges and universities worldwide in an effort to educate students (and parents) and attract them to cybersecurity programs.

It is more important than ever to spread awareness of the benefits of embarking on a cybersecurity career.

Indeed, as the old stereotypes of cybersecurity only relating to black hat activities and criminality slip away, it is now the time to promote the cybersecurity field and lure more students into entering STEM fields and becoming tomorrow's defenders.

Considering recent tech layoffs, it is also an opportunity for new public and educational partnerships to emerge and for individuals to upskill and retrain in the security field.

Initiatives include the U.S. National Security Agency's (NSA) Center of Academic Excellence in Cybersecurity **(CAE-C)**, which distinguishes academic institutions and provides grants to those that operate programs designed to improve the security of the U.S. national infrastructure.

Online, remote, and community college programs are crucial to grooming candidates for a range of roles in cybersecurity, whether as defenders, managers, risk analysts, product developers, or to become tomorrow's CISOs.

Cybercrime Magazine's **2023 Directory Of M.S. In Cybersecurity Programs At Universities In The U.S.** features hundreds of degree choices. Florida International University states that over **360,000 cybersecurity leadership roles** still need to be filled in the U.S. based on data from CyberSeek.

Considering the industry's momentum, Cybersecurity Ventures also expects the number of college and university graduates entering the cybersecurity sector to grow substantially through 2031.

Women in Security

According to Cybersecurity Ventures, women held 25 percent of cybersecurity jobs globally in 2022, up from 20 percent in 2019 and 10 percent in 2013.

After conducting in-depth discussions with industry leaders and reviewing third-party research, **we predict** that women will represent 30 percent of the global cybersecurity workforce by 2025. This figure is projected to reach 35 percent by 2031.

Women understand cyber. We need to encourage more women to enter STEM fields if we will tackle the existing skills shortfall effectively, especially with many businesses now adopting hybrid and remote practices, thereby decentralizing corporate resources, endpoints, and data.

Research has **suggested** that women entering STEM face long-standing obstacles, including unconscious and overt discrimination, disproportionate responses to errors, and delays in career progression.

Interestingly, similar levels of gender participation reveal themselves in the criminal underground – albeit without overt bias. It has been widely acknowledged that the majority of cybercriminals are male, but women now make up roughly **30 percent** of cybercrime forum members.

It may be the case that as a higher percentage of women join the industry as defenders, we will observe a comparable level of women opting for criminal routes, instead.

The **book** "Women Know Cyber: 100 Fascinating Females Fighting Cybercrime," and a **documentary** on women in the cybersecurity field, have contributed to the global movement around recruiting more women to our field.

Ron Green, executive vice president and chief security officer at Mastercard, sums it up best when it comes to attracting more women to our field when he says, "**You can't be what you can't see.**"

Promoting Diversity

As noted by **Microsoft**, "The defender community needs to be as diverse as the attackers we face."

This lesson applies to **women** and the **neurodiverse**, different ethnicities, and minority groups, for example **Black cybersecurity experts in the U.S.**

Cyberattacks are as diverse as the people who conduct them. Therefore, as **Craig Froelich**, CISO at Bank of America, told Cybersecurity Ventures, we need to have the same levels of diversity around the table.

Suppose organizations expand the inclusivity of their cybersecurity recruitment and training schemes. In that case, their staff can help them tackle defensive challenges from a variety of perspectives – and this can only be of benefit.

There is a pool of untapped talent available when organizations become more inclusive, and this is key to reducing the labor shortage.

Staff Retention

With 3.5 million cybersecurity jobs expected to remain open in 2025, organizations must retain their existing staff alongside developing new talent pipelines.

Research suggests that by 2025, nearly **50 percent** of CISOs will leave their roles, of which 25 percent will move down a different job path entirely.

Work-related stressors including staff shortages, budgetary constraints, insider risk, and the psychological pressure of shouldering a defensive role, may all contribute to essential employees leaving the field.

Furthermore, **47 percent** of cybersecurity incident responders say they've recently experienced burnout or extreme stress. Almost two-thirds have considered leaving their roles as a result.

Organizations must find enough talent to maintain an adequate security posture. However, retaining it is another matter entirely.

Business leaders have to become catalysts for cultural shifts beyond short wellness programs and extending vacation days to mitigate cybersecurity talent churn.

To do so, the pressures faced by existing cybersecurity teams and our CISOs must be better understood. Staff well-being and support should become priorities, especially considering the opportunities available elsewhere.

There are dozens upon dozens of roles in the cybersecurity industry, all requiring different skill sets and perspectives.

To manage **burnout** from the outset, placing people in roles based on their strengths is crucial. Leaders should also consider being flexible if an employee shows interest in a different facet of defense outside of their original posting.

Future View

The cybersecurity talent crunch is a serious challenge for modern-day organizations.

However, we are pleased to report movement in the right direction. Big tech, academic institutions, and non-profits are tackling the shortage with learning initiatives, scholarships, retraining, career advice, free resources, and courses aimed at colleges or earlier years. There is also a new and welcome interest in hiring women, minority groups, and the neurodiverse.

As understanding and comprehension of the importance of cybersecurity increases, we hope that organizations, from the top down, create more opportunities for new entrants and are willing to develop programs of value focused on hiring talent and retaining existing staff.

Cybersecurity Ventures predicts that by 2025, 35 percent of Fortune 500 companies will have board members with cybersecurity experience, and by 2031 that will climb to 50 percent.

Sponsored by eSentire

There is so much opportunity in the cybersecurity industry. We want more people to come into the industry but companies often require unrealistic experience. This results in unfulfilled jobs, sub-par company security and frustrated candidates who may give up. Companies need to hire from diverse sources. Internal IT is a great place to start but also consider candidates who may not have prior experience but demonstrate analytical thinking, a thirst for knowledge and a passion to do the job.

Greg Crowley,
CISSP, CISM, and CISO at **eSentire**

eSentire Inc., the Authority in Managed Detection and Response (MDR), protects the critical data and applications of 2000+ organizations in 80+ countries, across 35 industries from known and unknown cyber threats by providing Exposure Management, Managed Detection and Response and Incident Response services designed to build an organization's cyber resilience & prevent business disruption.

Founded in 2001, eSentire protects the world's most targeted organizations with 65 percent of its global base recognized as critical infrastructure, vital to economic health and stability. By combining open XDR platform technology, 24/7 threat hunting, and proven security operations leadership, eSentire's award-winning MDR services and team of experts help organizations anticipate, withstand, and recover from cyberattacks.

To learn more, visit **https://esentire.com**

2023 CYBERSECURITY JOBS REPORT is written by Charlie Osborne, Editor-at-Large for Cybercrime Magazine. Steve Morgan, founder of Cybersecurity Ventures contributed.

Cybersecurity Ventures
83 Main Street, 2nd Flr., Northport, N.Y. 11768
info@cybersecurityventures.com