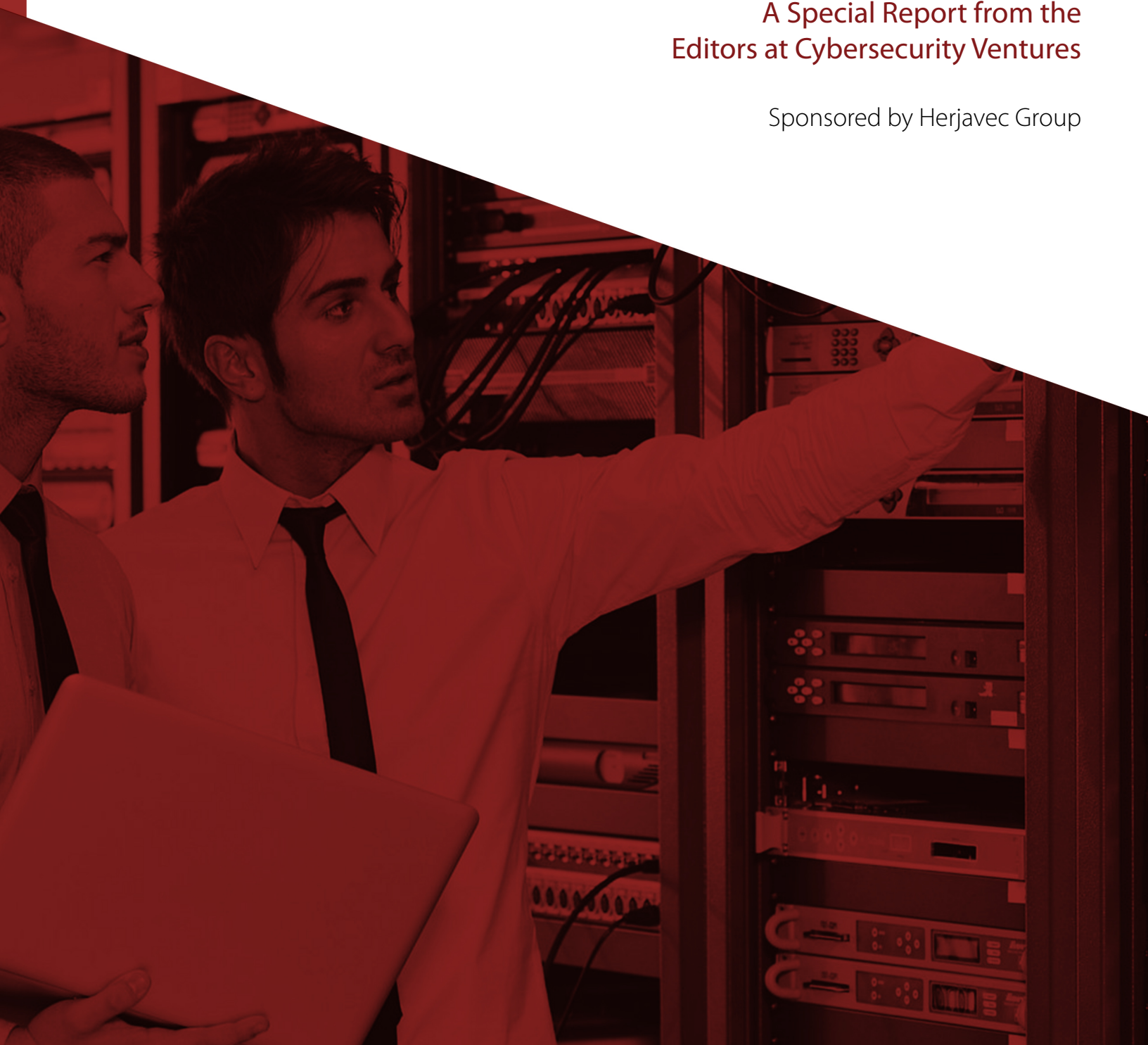
HERJAVEC GROUP

The 2019/2020 Official Annual Cybersecurity Jobs Report

A Special Report from the Editors at Cybersecurity Ventures

Sponsored by Herjavec Group



2019/2020 Cybersecurity Jobs Report

HERJAVEC GROUP

Cybersecurity Ventures predicts there will be 350 percent growth in open cybersecurity positions from 2013 to 2021.

The New York Times reports that a stunning statistic is reverberating in cybersecurity: Cybersecurity Ventures' prediction that there will be 3.5 million unfilled cybersecurity jobs globally by 2021, up from one million positions in 2014.

The cyber employment figure has been corroborated by hundreds of media outlets, including the world's largest, as well as industry associations, universities, governments, vendors, recruitment firms, and security experts, since our original report was published in May 2017.

Soon after our employment data was released, the World Economic Forum (WEF) republished an article with permission from Knowledge@Wharton, the online research and business analysis journal of the Wharton School of the University of Pennsylvania, which shared our report, and observed "nowhere is the workforce-skills gap more pronounced than in cybersecurity."

Earlier this year, the Harvard Business Review also shared our report, and summed up the plight: "The majority of chief information security officers around the world are worried about the cybersecurity skills gap, with 58 percent of CISOs believing the problem of not having an expert cyber staff will worsen."

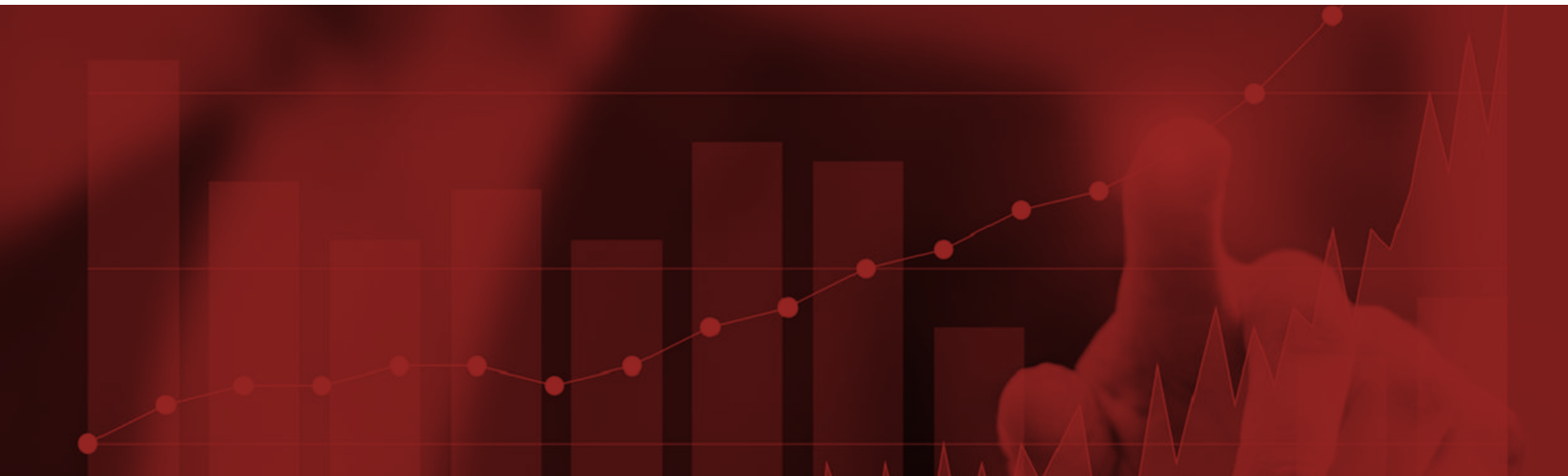
Cybersecurity Ventures arrived at our original estimation of unfilled positions after reviewing and synthesizing dozens of employment figures from the media, analysts, job boards, vendors, governments, and organizations globally. In 2019, we've conducted similar research, and we stand firmly behind the two-and-a-half-year-old prediction.

Over the eight-year period tracked, the number of unfilled cybersecurity jobs is expected to grow by 350 percent, from one million positions in 2013 to 3.5 million in 2021. And of the candidates who are applying for these positions, fewer than one in four are even qualified, according to the MIT Technology Review.

Despite industry-wide efforts to reduce the skills gap, the open cybersecurity headcount in 2021 will be enough to fill 50 NFL stadiums. A Forbes Technology Council post states that the number would be in the top 100 for the size of work populations of countries worldwide — not just industries.

Every IT position is also a cybersecurity position now. Every IT worker, every technology worker, needs to be involved with protecting and defending apps, data, devices, infrastructure, and people.

"It's a full-on war for cybertalent," one industry veteran who specializes in recruiting and placing senior-level information security executives told the Los Angeles Times.



Robert Herjavec, Founder & CEO of Herjavec Group, said, "Unfortunately the pipeline of security talent isn't where it needs to be to help curb the cybercrime epidemic. Until we can rectify the quality of education and training that our new cyber experts receive, we will continue to be outpaced by the Black Hats.

"We put a significant emphasis on training and certification here at HG because we recruit from all fields and we want our people to advance, internally within the company. I'm looking for a curious person who can analyze patterns, investigate data and develop technical skill. We've recruited English majors, political science grads and yes of course computer science or cybersecurity students. It all comes down to your critical thinking skills and your aptitude to learn."

"There is a zero-percent unemployment rate in cybersecurity and the opportunities in this field are endless," continued Herjavec. "Gone are the days of siloed IT and security teams. All IT professionals need to know security – full stop. Given the complexity of today's interconnected world, we all have to work together to support the protection of the enterprise."

Numerous pundits from industry associations and vendors have chimed in on the cybersecurity jobs dilemma, with adjustments to shortfalls in their previous estimates, which now align more closely with Cybersecurity Ventures' steady forecast.

ISC(2), an international, nonprofit membership association for information security leaders, produced research in 2018 which estimated the cyber worker shortage at nearly 3 million — on the heels of a report they put out just a year earlier, which stated a drastically lower 1.8 million figure by 2022.

Members of the ISC(2) leadership team recently posted a blog on their website which states "the cybersecurity skills shortage is expected to result in 3.5 million unfilled positions by 2021" (according to Cybersecurity Ventures via Forbes) — which underscores ISC(2)'s alignment to our research.

"By Cybersecurity Ventures' predictions, and we agree from everything we see, there will be 3.5 million unfilled cybersecurity jobs in the next couple of years worldwide," said Mark Aiello, a cybersecurity recruiting expert and representative for the eastern Massachusetts chapter of ISC(2) at a recent cybersecurity conference held in Boston.

Our estimate is firmly solidified as the de facto figure that our industry and the media relies upon for projected cybersecurity job openings.

A Forbes Business Development Council post asserts that if you aren't prioritizing hiring or training for IT security in 2019, then it's time to rethink your company's core priorities. If you agree, then read on…

The editors at Cybersecurity Ventures have compiled the most important facts, figures, statistics, and predictions to help frame the global cybersecurity labor shortage, and what is being done in an attempt to close the gap.

Unfilled Jobs

No matter how you crunch the numbers, there's a huge need for cybersecurity workers over the next decade.

- Out of the 3.5 million open cybersecurity positions expected by 2021, Cybersecurity Ventures estimates more than 2 million openings will be in the Asia-Pac region, and nearly 400,000 will be in Europe.
- The U.S. has a total employed cybersecurity workforce consisting of 715,000 people, and there are currently 314,000 unfilled positions, according to Cyber Seek, a project supported by the National Initiative for Cybersecurity Education (NICE), a program of the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce.
- Members of the CNBC Tech Council put the number of U.S. technology job openings at 700,000 to 1 million over the past 12 to 24 months. Based on those figures, cybersecurity positions made up 32-45 percent of all U.S. tech job openings.
- At the end of 2018, there were more than 26,000 openings for cybersecurity analysts in the U.S.
- Cybersecurity isn't alone in the labor crunch, although it's one of the hardest hit STEM fields. Between 2017 and 2027, STEM jobs will grow 13 percent, compared to 9 percent for all other jobs. However, it was estimated that in 2018, 4 million STEM jobs in the U.S. went unfilled.

U.S. Metros

There are many new initiatives across the U.S. that are aimed at bolstering our nation's future pipeline of cybersecurity candidates.

- Government Technology recently reported that Massachusetts has more than 9,000 open cybersecurity jobs. The MassCyberCenter is looking to boost the state's cyber resilience and economic growth and to partner with businesses, academia and the public sector to train new cybersecurity workers.
- To develop the cyber workforce of the future, the New York City Economic Development Corporation (NYCEDC) launched Cyber NYC, which is supposed to catalyze 10,000 cyber jobs, help fuel new startups, and protect the city's anchor employers. The project is among the nation's most ambitious cybersecurity initiatives, which over the next decade could transform New York City into a global leader of cybersecurity innovation and job creation.
- The New York metro area (NY-NJ-CT) has the second-largest absolute number of cybersecurity job openings – roughly 20,000.
- Employers in the Philadelphia area struggled to fill more than 10,000 open roles requiring cybersecurity skills last year. In Philadelphia, the biggest skill shortages fall within the following areas: security analysis and investigation, application security, and cloud computing security.
- The population of cyber engineers and analysts throughout the Washington D.C. Beltway is 3.5 times as big as the rest of the U.S. combined.
- With more than 150,000 cyber-related engineering and data science professionals, Maryland has the number one cyber workforce in the world, and leads the U.S. in cyber employment for classified nation-state jobs. Maryland also has the largest concentration of university-trained cyber engineering graduates in the world.
- There are currently over 15,000 open cybersecurity jobs in Maryland — and that number is growing by the day, according to the Maryland Chamber of Commerce.
- The Northern Virginia Technology Council noted that employers in the region are struggling to find candidates who have both the technical and soft skill competencies they need. Employers cite soft skills deficiencies as their primary pain point outside of the obvious shortage of qualified candidates.
- The top five states for cybersecurity jobs are Virginia, Texas, Colorado, New York and North Carolina — where average annual salaries for cybersecurity roles exceed $100,000, according to a DarkReading analysis that analyzed data from a recent report.

2019/2020 Cybersecurity Jobs Report

HERJAVEC GROUP

- The Georgia Cyber Center, a $100 million facility, the country's largest cyber investment of its kind by a state government, is intended to train the IT security workforce of the future.
- The University System of Georgia signed an agreement with the U.S. Army Cyber Center that will allow active duty and reserve military members to work toward a degree in cyber fields at several of Georgia's universities during their service. The Army intends for the program to help fill over 11,000 open cyber jobs in the state, both inside and outside the armed forces.
- The Cyber Innovation Center in Bossier City, Louisiana, which has new Homeland Security funding, expects to broaden its cyber skills preparation to 10 million students and 50,000 teachers in K-12 across the U.S — which should eventually bolster the pipeline of young cyber workers.
- Tech employment in Chicago grew by nearly 6,000 jobs last year, and cybersecurity analyst is one of the top 3 tech positions in the windy city.
- San Antonio is home to the nation's second-largest concentration of cybersecurity experts. With a pipeline of cybersecurity talent from San Antonio's K-12, up through top higher education programs and advanced military backgrounds, the city, a.k.a. Cyber City, USA, is preparing for jobs employers need to fill today and in the future.
- Texas has the most cybersecurity growth potential in the U.S., according to Business Facilities' 15th Annual Rankings Report.
- Arizona, which the Federal Trade Commission ranked as one of the top 10 in cybersecurity, has roughly 7,000 cybersecurity job openings.
- San Diego, home to the U.S. Space and Naval Warfare Systems Command (SPAWAR), and home to more than 150 cybersecurity companies, has around 8,450 cybersecurity jobs, which is up by 11 percent from three years ago, according to the region's Cyber Center of Excellence.
- California has 50 companies (33 percent) named on Cybersecurity Ventures' Hot 150 Cybersecurity Companies To Watch In 2020 list, the bulk of whom are located in or in close proximity to Silicon Valley. These plus hundreds of others in this region have created an extraordinarily competitive market for sales, marketing, and engineering talent.

International

Help Wanted: Cybersecurity experience preferred. This is the consistent theme across regions globally.

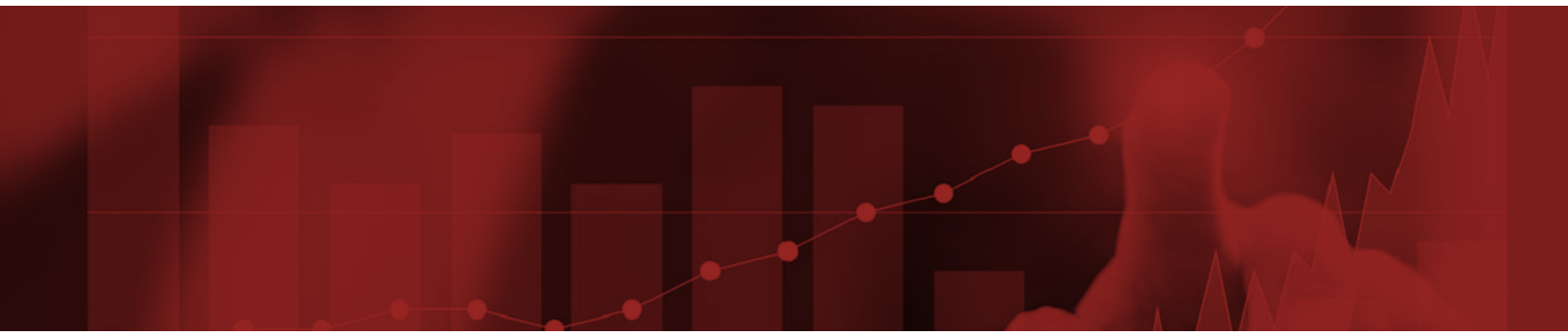
- India — by far — had the largest growth in cybersecurity job openings from 2017 to 2018, followed by Sweden, Ireland, Italy and the UK.
- The National Association of Software and Services Companies (NASSCOM) estimates that India — a country with a population of approximately 1.34 billion people — alone will need 1 million cybersecurity professionals by 2020 to meet the demands of its rapidly growing economy.
- Skill shortages in Europe are damaging the growth prospects of companies and the continent's economy, according to an EY survey. The most alarming talent shortages are in digital skills, with cybersecurity (48 percent) identified as one of the scarcest skills.
- A recent parliamentary inquiry found the cybersecurity worker shortage is "verging on a crisis" in the UK. The joint committee on the national security strategy's review found even the National Cyber Security Centre (NCSC), the government body charged with providing cybersecurity advice and support, faces a constant challenge to recruit the expertise it needs.
- Ireland's skills gap continues to increase, particularly in the area of cybersecurity, where there's growing demand for roles year on year. The country is unable to keep up with its 18 percent increase in the demand for cybersecurity roles.
- Israel, the world's no. 2 exporter of cyber technology and one of the top 10 global cybersecurity hubs for 2019, is experiencing a worker shortage that is the most significant problem the sector is facing today. This shortage is causing local salaries to surge and is pushing firms to seek workers abroad, according to a recent report by Start-Up Nation Central and the Israel Innovation Authority.
- A report coming out of Australia found that 88 percent of IT decision-makers believe there is a shortage of cybersecurity skills within their own organization, but also nationally.
- To address its cyber skills shortage in South Africa, Absa has collaborated with the Maharishi Institute (MI) to set up a Cybersecurity Academy. The program is aimed at empowering marginalized youth, who would otherwise not have had access to tertiary education. The learners who participate become certified cybersecurity analysts.
- Nigeria has a chronic shortage of cybersecurity workers. With an estimated population close to 200 million, the number of certified cybersecurity professionals in Nigeria was a mere 1,800 as of last year. Microsoft has called for safer online community in Nigeria for improved economic growth.
- Research from Deloitte shows a lack of talent is being felt across corporate Canada. Critical roles are going unfilled, and it's expected that organizations across Canada will need to fill an estimated 8,000 additional cybersecurity positions by 2021.
- To help grow a security-trained workforce, the Cisco Networking Academy has partnered with 1,550 academies and 3,800 instructors to provide cybersecurity training across Latin America. As of last year, some 1.6 million had already completed the coursework.

Trends

If there's one trend that everyone can agree on, it's that cybersecurity is a fast-growing market with tremendous career opportunities.

- The cybersecurity unemployment rate is at zero percent in 2019, where it's been since 2011.
- Cybersecurity Ventures forecasts that 100 percent of large corporations (Fortune 500, Global 2000) globally will have a CISO or equivalent position by 2021 (up from 70 percent in 2018), although many of them will be unfilled due to a lack of experienced candidates.
- The U.S. Bureau of Labor and Statistics projects that employment for information security analysts will grow at 32 percent between 2018 and 2028, which is higher than the average for all other occupations.
- Readers Digest named cybersecurity project managers and blockchain developers on its list of the 21 most in-demand jobs for 2020.

- Jobs requesting public cloud security skills remain open 79 days on average — longer than almost any other IT skills, according to Cyber Seek.
- A Forbes HR Council post observes that 74 percent of companies recently surveyed said that the skills shortage is impacting their business, including the ability to keep their information secure.
- Tech executives on the CNBC Technology Executive Council said it has become harder to fill IT and cybersecurity positions, so candidates with liberal arts degrees, or no college degree, are now being hired.
- CISSPs (Certified Information Systems Security Professionals) rank sixth out of the top 20 fastest-growing skills for freelancers.
- According to a DarkReading report published last year, only 14 percent of IT security managers felt there were enough cybersecurity professionals in the field with the needed skills to hunt down and respond to threats.
- The cybersecurity labor shortage is felt most acutely in the government workforce. Federal agencies, such as the Department of Defense — which houses both the National Security Agency and the U.S. Cyber Command — have a hard time competing with the private sector for top cyber talent.
- One of the 5 biggest trends in the job market is a rise in cybercrime, which is spurring growth in security skills, according to CNBC.
- Debby Carreau, CEO & founder of Inspired HR and a member of the CNBC-YPO Chief Executive Network, lists cybersecurity as one of five hot industries that are a safe bet for a career that's future-proof.
- Retention is a major issue for employers. According to a McAfee survey of 950 cybersecurity managers and professionals at organizations with 500 or more employees in the U.S., U.K., Germany, France, Singapore, Australia, and Japan, a full 89 percent of respondents would consider leaving their roles if offered the right type of incentive.



Youth Movement

We need to encourage and nurture our K-12 and college students to become future cyber fighters.

- One of the keys to building a future cybersecurity workforce is instilling enthusiasm for STEM and cybersecurity at an early age. The first-ever national Cybersecurity badges for girls in grades K–12 were announced by the Girl Scouts of the USA in 2017 and there has been strong industry support for the initiative.
- The National Security Agency has been training kids to root out cybercriminals since 2014. This past summer through a program called GenCyber, the N.S.A. ran 122 cybersecurity camps — named Camp Cryptobot — across the country, in order to generate a future pipeline of cyber workers.
- In one report, across 24 states, only 35 percent of high schools in the U.S. teach computer science — much less focus specifically on cybersecurity — despite the fact that 90 percent of parents want computer science education for their children, according to Ralph P. Sita, co-founder and CEO at Cybrary, a provider of free online cybersecurity training.
- According to McAfee's Winning the Game report, 92 percent of cybersecurity managers say gamers possess skills that make them suited to a career in cybersecurity — and 75 percent would consider hiring a gamer even if that person had no cybersecurity training or experience.

- By 2025, millennials will make up 75 percent of the global labor force — and more than 70 percent of the ethical hacker community is already under the age of 30. Organizations therefore need to tap into this community in order to build their cybersecurity workforce.
- Just 4.2 percent of federal cybersecurity workers are aged 30 and under. These people are charged with protecting the country's digital infrastructure via jobs in such departments and agencies as the Department of Defense, CIA, Federal Election Commission and Department of Energy (which designs, tests and creates nuclear weapons for the U.S., among other tasks).

Compensation

Cybersecurity is a highly respected and well-paying occupation, from entry-level positions up to chief information security officers (CISOs).

- The top 10 percent of cybersecurity analysts make over $117,000 per year, while the median annual salary is $76,000.
- New data indicates that of all IT jobs, cybersecurity engineers — with an average annual salary of $140,000 — were the highest paying and most recruited heading into 2019.
- For the top coders with leadership and cybersecurity skills — a rare breed — salaries exceed $225,000. In some companies, this position pays more than it does to the CISO. Software plus "soft skills" equals big pay for aspiring programmers with a senior management role in their sights.
- The second-highest paying tech job in 2019 is a CISO, with a salary range of $175,000 to $275,000. Fortune 500 corporations in big cities pay as much as $380,000 to $420,000 annually, and more, to their CISOs, much higher than the average range for the position in mid-sized companies, government agencies, and academia.
- At the top of the cybersecurity food chain (ranked by pay), there are a small number of CISOs earning 7-figure annual pay packages.
- Flaws in software code, which create vulnerabilities, have created a burgeoning bug bounty economy with big payouts to elite freelancer hackers. Some of them earn more than $500,000 a year. But, that's a far cry from the average take-home pay for most bug bounty hunters who are self-employed part-timers with no guaranteed income.

Women in Cybersecurity

Women know cyber, and we need more of them in the cybersecurity industry. Their talents and contributions are essential to the well being and safety of the world.

- Cybersecurity Ventures predicts that women will represent 20 percent of the global cybersecurity workforce by the end of 2019. This recalculates a 6-year old figure based on a limited survey that concluded women held just 11 percent of cybersecurity positions.
- Research firm Forrester predicts that the number of women CISOs at Fortune 500 companies will rise to 20 percent in 2019, compared with 13 percent in 2017. This is consistent with new research from Boardroom Insiders which states that 20 percent of Fortune 500 global CIOs are now women — the largest percentage ever.
- Women in the cybersecurity field are trending up in Israel, the world's second-largest country in terms of cybersecurity investment. In 2018, TechCrunch reported that for the most recent year tracked, 15 percent of newly established Israeli cybersecurity startups had a female founder, an increase from 5 percent the previous year.
- 91 percent of women in cybersecurity have a bachelor's degree, and 20-25 percent of them have an MBA or master's degree. 5 percent have a Ph.D., and 2 percent have no degree.
- A new book published by Cybersecurity Ventures — "Women Know Cyber: 100 Fascinating Females Fighting Cybercrime" — is intended for students, parents, and educators, in order to spur more interest in our field.

Certifications

Here are 10 hot security certifications for IT workers in 2020, compiled by the editors at Cybercrime Magazine:

- Certified Ethical Hacker (CEH) — A Certified Ethical Hacker is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system(s).
- Certified in Risk and Information Systems Control (CRISC) — CRISC is the only certification that prepares and enables IT professionals for the unique challenges of IT and enterprise risk management, and positions them to become strategic partners to the enterprise.
- Certified Information Privacy Professional/US (CIPP/US) — Backed by ANSI/ISO accreditation, a CIPP/US credential delivers higher earning potential and increased promotion opportunities because it shows you have a strong understanding of U.S. privacy laws and regulations.
- Certified Information Security Manager (CISM) — CISM means higher earning potential and career advancement. Recent independent studies consistently rank CISM as one of the highest paying and sought after IT certifications.
- Certified Information Systems Auditor (CISA) —Enhance your career by earning CISA — world-renowned as the standard of achievement for those who audit, control, monitor and assess information technology and business systems.
- Certified Information Systems Security Professional (CISSP) — Accelerate your cybersecurity career with the CISSP certification. Earning the CISSP proves you have what it takes to effectively design, implement and manage a best-in-class cybersecurity program.
- Cisco Certified Network Associate Security (CCNA) — With a CCNA Security certification, a network professional demonstrates the skills required to develop a security infrastructure, recognize threats and vulnerabilities to networks, and mitigate security threats.
- Cisco Certified Network Professional Security (CCNP) — This certification is aligned to the job role of the Cisco Network Security Engineer responsible for security in routers, switches, networking devices and appliances, as well as choosing, deploying, supporting and troubleshooting firewalls, VPNS, and IDS/IPS solutions for their networking environments.
- CompTIA Security+ — CompTIA Security+ is the first security certification IT professionals should earn. It establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs.
- Computer Hacking Forensics Investigator (C|HFI) — Computer investigation techniques are being used by police, government and corporate entities globally and many of them turn to EC-Council for their Computer Hacking Forensic Investigator CHFI Certification Program.

Job Seekers

Five resources for cybersecurity job seekers:

- 50 Cybersecurity Titles That Every Job Seeker Should Know About, compiled by the editors at Cybercrime Magazine.
- 20 Coolest Cybersecurity Jobs, compiled by SANS Institute
- Information Security Analyst Salaries by State, based on BLS data, from UC Berkeley School of Information.
- Pink Slips To Million Dollar Salaries: Are CISOs Underappreciated Or Overpaid? CISO compensation observations from the editors at Cybercrime Magazine
- Top 5 Cybersecurity Jobs That Will Pay $200,000 To $500,000 In 2019, from the editors at Cybercrime Magazine

The editors at Cybercrime Magazine maintain a catalog of cybersecurity career related stories that feature research from Cybersecurity Ventures. This is a useful resource for job seekers, hiring managers, HR chiefs, search firms, recruiters, and market watchers.

"30 years ago, I had no idea a career in cybersecurity was even possible. Today it's the hottest industry to be a part of and the resources are available, at your finger tips, to learn more and engage," says Herjavec Group's Robert Herjavec. "This is an ever evolving industry, and the demand for incredible talent with varying skills – from coding, to analysis, to hunting to technical expertise in a particular technology discipline, to consultation… it isn't slowing down anytime soon. What are you waiting for?"

About the Author

Steve Morgan is Founder and Editor-In-Chief at Cybersecurity Ventures. He oversees all of the editorial for Cybersecurity Ventures which includes our research, quarterly and annual reports, and directories.

About Cybersecurity Ventures

Cybersecurity Ventures is the world's leading researcher and publisher covering the global cyber economy. Our firm delivers cybersecurity market data, insights, and ground-breaking predictions to a global audience of CIOs and IT executives, CSOs and CISOs, information security practitioners, cybersecurity company founders and CEOs, venture capitalists, corporate investors, business and finance executives, HR professionals, and government cyber defense leaders.

For more information, visit http://www.cybersecurityventures.com/

About Herjavec Group

Dynamic entrepreneur Robert Herjavec founded Herjavec Group in 2003 to provide cybersecurity products and services to enterprise organizations. We have been recognized as one of the world's most innovative cybersecurity operations leaders, and excel in complex, multi-technology environments. Our service expertise includes Advisory Services, Technology Architecture & Implementation, Identity Services, Managed Security Services, Threat Management, and Incident Response. Herjavec Group has offices and Security Operations Centers across the United States, United Kingdom, and Canada.

For more information, visit **www.herjavecgroup.com.**

Follow Us
Herjavec Group
@HerjavecGroup