Cybersecurity JOBS GUIDE

A WGU and LinkedIn Collaboration

WGU LinkedIn

> Cybersecurity is in dire need of really good people.
>
> **— Randall Frietzsche**

Have you ever wondered what it would be like to be a cybersecurity professional? Better yet, do you know how to get there? Do you have to know how to program, take apart malware, be a master at ethical hacking, and have experience with penetration testing? Actually, you probably already have what it takes: **curiosity**.

While many cybersecurity professionals have technical skills, you might be surprised to hear that many of them got there from other fields such as law enforcement, customer service, and project management. They made the switch to cybersecurity armed with nothing more than their curiosity, a drive to learn, and some combination of university degrees and certifications.

As the field expands, these areas of expertise become even more crucial—and more in-demand. In fact, hundreds of thousands of cybersecurity jobs go unfilled every year because employers can't find the talent they are looking for.

To illustrate the magnitude of this crisis, WGU teamed up with LinkedIn, one of the largest online networks of professionals, to run a targeted analysis of the cybersecurity job market. Unsurprisingly, the study confirmed what we already know: the demand for cybersecurity professionals is increasing and shows no signs of slowing down. Luckily, you don't have to be a computer genius to enter the field. With the right attitude, the right education, and your natural inclination to learn, you can become a cybersecurity professional.

"Cybersecurity is in dire need of really good people," said Randall "Fritz" Frietzsche, Chief Information Security Officer (CISO) for Denver Health and a graduate of WGU's Master of Cybersecurity Security and Information Assurance program. "We find that we have more of a need than we have people available out there, and it becomes almost impossible to find someone to fill an open role, because everybody who is qualified already has a job."

Job Market Overview, Shortages, and Drivers of Growth

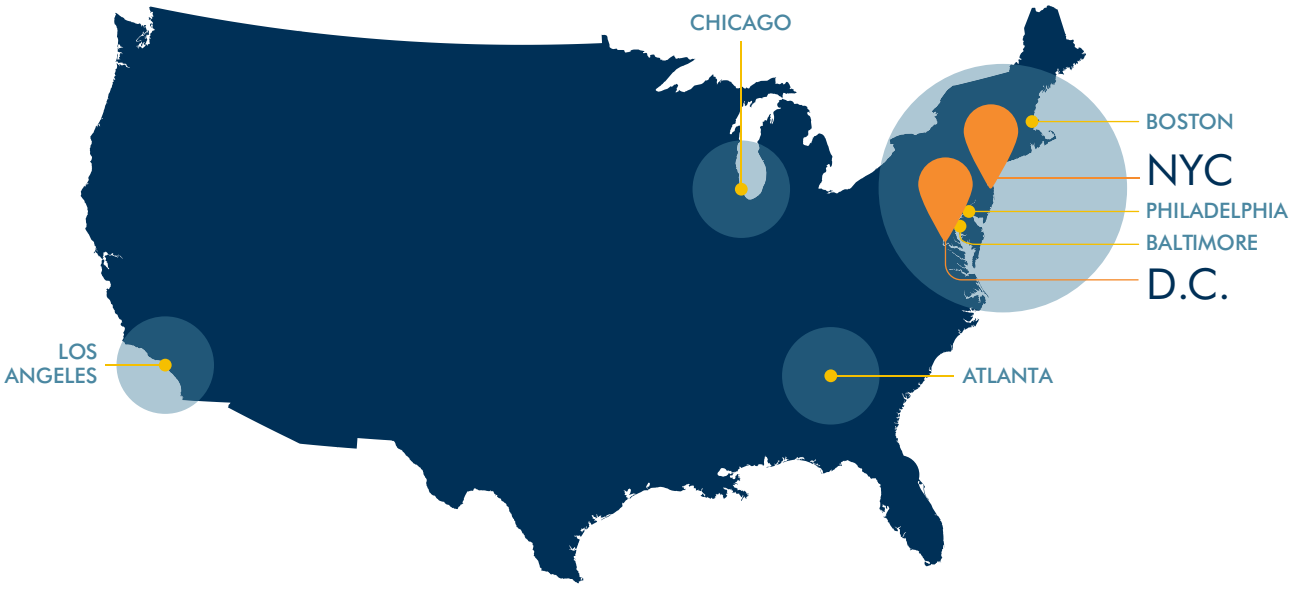
As a subdomain of IT, cybersecurity pays some of the highest salaries and has tremendous growth potential. But the industry is facing a massive skills shortage as the demand for qualified professionals continues to grow.

YEAR-OVER-YEAR INCREASE IN CYBERSECURITY ACTIVE JOB LISTINGS

YEAR	ENTRY	ASSOCIATE	MID-SENIOR+	ALL JOBS
2014-2015	+20%	+114%	+104%	**+50%**
2015-2016	+83%	+72%	+71%	**+78%**
2016-2017	+50%	+63%	+118%	**+58%**

Source: LinkedIn

In some U.S. metropolitan areas, this shortage of skilled workers has reached an alarming level. For example, there were over 25,000 cybersecurity job postings in the Washington D.C. area in 2017, yet LinkedIn only identified about 7,200 cybersecurity professionals located in the region. That means there were 3.6 potential job offers for each qualified professional. The Greater New York City area saw the same ratio, with nearly 9,000 job openings and only about 2,500 cybersecurity professionals in the region. In fact, many metro areas showed similar shortages, including Baltimore, Chicago, Boston, Atlanta, Philadelphia, and Los Angeles, which all had over 2.8 times more job openings than qualified cybersecurity professionals living there.



> It's more enticing to go after 10,000 small businesses than one whale.
>
> **— Brandon Knotts**

Where is all this demand coming from? Of course, most big companies have cybersecurity departments, but many small and medium-sized organizations are also realizing that their business runs on data and depends on information technology (IT). They're also finding that new rules and regulations, such as the European Union's (EU) General Data Protection Regulation (GDPR), are requiring them to improve their data protection strategies.

"Some of our smaller clients say, 'Why in the world would we spend any money on security? We're a small town newspaper,'" noted Brandon Knotts, CEO of IT solutions and staffing firm Dash2. "In the past, who would target a company like that? You'd go after companies like Walmart or Sony. But now, because of automation that allows hackers to target larger numbers of businesses, it's more enticing to go after 10,000 vulnerable small to medium-sized businesses than one whale."

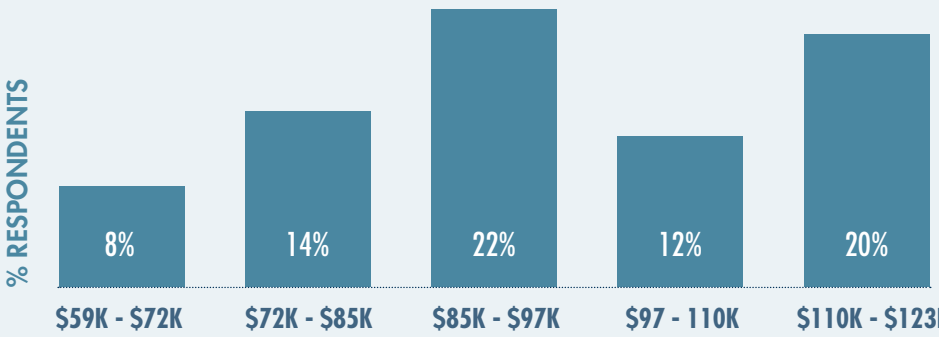
And don't forget about cyberattackers, who are dedicated to trying to infect machines, hold data for ransom, and siphon money right out of bank accounts. These threats are becoming more sophisticated and widespread with the rise of the Internet of Things (IoT), artificial intelligence (AI), and other emerging technologies that make valuable data increasingly accessible to malicious actors.

"Securing your business is not a one-and-done investment, and more companies are beginning to realize this," said Greg Larsen, Director of IT Services at Dash2 and a graduate of WGU's MBA program. "Hackers know that many companies don't do the foundational-level work, so they automate these attacks to target small to mid-sized businesses."

As the technology landscape continues to evolve, these threats will only multiply and grow increasingly complex. So too will the cybersecurity skills shortage, which is why the search for qualified talent is more urgent than ever for businesses of all sizes.

The Cybersecurity Lifestyle: Great Salaries, Cool Job Duties

There is an extremely high demand for cybersecurity professionals and a shortage of qualified candidates. Partially due to this high demand, cybersecurity salaries are higher than many other IT jobs. In fact, according to data from LinkedIn, the median base salary of a cybersecurity professional in the U.S. is about $92,500 per year.



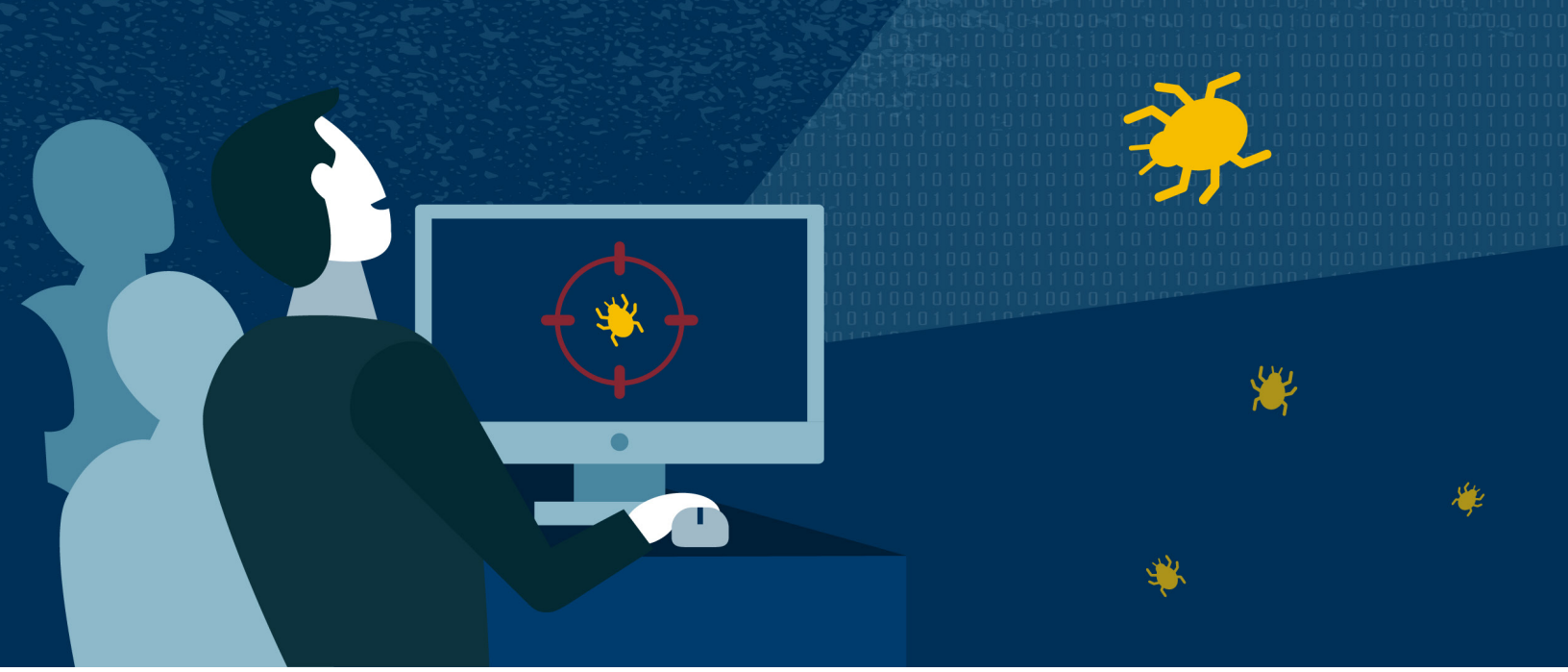
Source: LinkedIn

But are all these jobs reserved for senior-level professionals, or is there room for newcomers? LinkedIn data from 2017 shows 53 percent of cybersecurity-related job listings were for entry-level positions, while 40 percent were for associate-level roles and 7 percent for mid- to senior-level positions.

As companies expand their security teams, there will also be room to grow into mid- and top-level management positions over time. By all accounts, now is a good time to start thinking about a cybersecurity career.

Cybersecurity is about protecting and serving the organization, and keeping the business running. It makes sense, then, that many people in the field have transitioned from military and law enforcement careers. Cybersecurity professionals often talk about a sense of mission and the satisfaction they get from protecting their colleagues and customers, and the data and systems that run the business.

53%
of cybersecurity-related job listings were for entry-level positions.



> We're all fighting the same good fight.
>
> **— Randall Frietzsche**

"What really makes people shine is when it's clear that they love this—they eat, sleep, and breathe it," said Greg Larsen, Director of IT Services at Dash2 and a graduate of WGU's MBA program. "That's going to make you the absolute best candidate that we can possibly find."

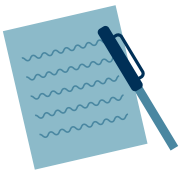
This sense of mission makes for a highly collaborative, collegial environment of professionals who are fighting a common enemy. "There's really no competition in cybersecurity," said Randall "Fritz" Frietzsche, Chief Information Security Officer (CISO) for Denver Health and a graduate of WGU's Master of Cybersecurity Security and Information Assurance program. "We're all fighting the same good fight."

There are a number of different cybersecurity roles and job titles. Some people have more business-facing or analytical responsibilities, often reporting and translating cyber issues into business-level concerns, while others build, test, and configure systems. The former tend to have "analyst" in their job description, and the latter tend to be called "engineers." According to LinkedIn, the most common job titles related to cybersecurity are information security analyst, network security engineer, information security engineer, cybersecurity analyst, information security specialist, cybersecurity engineer, and senior versions of those roles.

While many of these cybersecurity positions require specific technical skills, others also rely on soft skills, such as customer service, communication, and project management. This opens the door to the profession to candidates with a variety of backgrounds and skill sets.

Required Skills and Experience

What's the best way to get started in a cybersecurity career, and how valuable are certifications compared to a traditional four-year degree?



According to LinkedIn, 71 percent of professionals who transitioned from other careers into entry-level cybersecurity jobs had a bachelor's degree. That number rose to 73 percent for associate-level roles and 76 percent for mid- to senior-level positions. This data shows that a four-year degree is valuable for professionals trying to transition into cybersecurity. In their previous careers, according to LinkedIn, some of these people held titles such as network engineer, network administrator, consultant, intern, project manager, and manager or program manager, but LinkedIn's data suggests, above all, that there is no single pathway to cybersecurity, and that the majority come to the profession from a wide variety of different backgrounds.

	% OF TOTAL CYBERSECURITY PROFESSIONALS	HAS BA/ BS DEGREE
ENTRY	51%	71%
ASSOCIATE	39%	73%
MID-SENIOR	10%	76%

Source: LinkedIn

What if you're already working in cybersecurity? Would a formal degree help with a promotion? According to LinkedIn, of the people who were promoted in the past two years, over 70 percent of entry- and associate-level employees and 77 percent of mid- to senior-level employees had traditional degrees. For middle and senior positions, 77 percent of those who were promoted in the past two years had a four-year degree.

What about certifications? Like a degree, a certification is highly valuable because it shows that you've mastered a set of critical technical skills, and that you are committed to furthering your education, investing in yourself, and challenging yourself. The more credible the source is, the more valuable a certification will be. And at the end of the day, the best candidates will have some combination of formal education, certifications, and innate skills.

> There are many paths that lead to a successful career in cybersecurity.

But while technical skills are certainly important in the cybersecurity field, some positions rely just as heavily on soft skills such as customer service, communication, and project management. In fact, according to LinkedIn, 28 percent of entry-level cybersecurity professionals listed customer service as a skill. "If you're a help desk person, a desktop person, or even a server/network type of a person, the first step is to really recognize that you're already doing security," said Randall "Fritz" Frietzsche, Chief Information Security Officer (CISO) for Denver Health and a graduate of WGU's Master of Cybersecurity Security and Information Assurance program.

Ultimately, there are many paths that lead to a successful career in cybersecurity. For those currently in IT, you are closer than you think. With the right degree, you can leverage the security work you already do to gain new knowledge and bolster your cybersecurity aptitude. For aspiring cybersecurity professionals transitioning from nontechnical careers, IT isn't the only path. Anyone with strong soft skills, people skills, or experience in product management can make the switch and flourish in a cybersecurity career. As Frietzsche put it, "If you can learn to drive a forklift, you can learn security, as long as you have an aptitude for it, and an interest and a passion for it."

Put simply, the cybersecurity industry is in dire need of candidates who are committed to professional development, willing to work, and eager to learn. And it's safe to say that this is only the beginning for the rise in cybersecurity roles. Luckily, the field is extremely welcoming to professionals from a broad range of backgrounds and skill sets. So if you're looking for a mission-driven profession that provides a collegial environment, the cybersecurity field might be right for you.

About
Western Governors University

Western Governors University (WGU) is a nonprofit online university with more than 100,000 graduates from all 50 states. Nationally respected and regionally accredited by the Northwest Commission on Colleges and Universities, WGU was named a "Best Value School" by University Research & Review for four consecutive years.

WGU is also a program member of the Microsoft IT Academy and the National Cyberwatch Center and a 2016 CODiE award winner from the Software & Information Industry Association.

WGU's online degree programs in cybersecurity are closely aligned with the National Initiative for Cybersecurity Education (NICE) and were designed specifically with input from cybersecurity experts and leading IT employers to meet the most recent U.S. Department of Homeland Security (DHS) and National Security Agency (NSA) guidelines.

With WGU's timely, relevant, and practical curriculum, students are able to earn cybersecurity certifications even before they complete their degree programs. How quickly you progress in your program is driven by your ability to prove mastery of the course material.

Contact a WGU Enrollment Counselor today at **866.225.5948** for an assessment of how your work experience and prior college credits can be applied toward your cybersecurity degree.

wgu.edu

WGU