

Recruiting Watchers for the Virtual Walls

The State of Cybersecurity Hiring

June 2019





Table of Contents

1.	Introduction and Methodology	pg 4
2.	Findings	pg 8
3.	Implications	pg 18
4.	Appendix	pg 22
5.	Resources and Acknowledgements	pg 24

1.

Introduction & Methodology

Six years ago, Burning Glass Technologies set out to answer a basic question about the growing threat of cyberattack: Did American employers have the cybersecurity talent they needed to face the problem?

Today the threat remains as potent as ever—and so is the persistent cybersecurity talent shortage. There have been major efforts to increase the supply of cybersecurity workers. But demand has increased as well, which means cybersecurity talent is still expensive and hard to find.

For example, federal data shows the number of postsecondary programs in key cybersecurity areas has increased 33%, and the number of conferrals rose 44% between 2013-17.¹ Yet one key indicator of supply and demand, the ratio of currently employed cybersecurity workers to job openings, has hardly budged since 2015. In other words, the pool of available talent has remained proportionally the same.

One reason for this is the very fact that cybersecurity is now more widely considered a critical function. Demand for security skills, once limited primarily to government and the defense industry, has spread throughout the economy.

Over time, we can see both the changing priorities and tactics of cybersecurity reflected in hiring patterns. Overall, the field is emphasizing deploying automation and managing risk more effectively. That is partly

in the belief that these tactics will be more effective in preventing breaches—but it is no coincidence that they also alleviate the need for hard-to-hire human workers. In addition, projections show that the next generation of cybersecurity workers will need skills in cloud security and the Internet of Things.

Burning Glass Technologies has been tracking the cybersecurity job market since 2013, both in a series of reports and on the website [Cyberseek.org](https://www.cyberseek.org). Based on our database of nearly one billion current and historical job postings, Burning Glass has built a definition of the cybersecurity job market that includes all job openings with cybersecurity-related job titles, skills, or certifications. This enables a more comprehensive and granular view of the cybersecurity jobs landscape.

Key findings from this report:

- The number of cybersecurity job postings has grown 94% since 2013, compared to only 30% for IT positions overall. That's over three times faster than the overall IT market.
- Cybersecurity jobs account for 13% of all information technology jobs. On average, however, cybersecurity jobs take 20%

¹ National Center for Education Statistics IPEDS database for programs in Computer and Information Systems Security/Information Assurance and Cyber/Computer Forensics and Counterterrorism. <https://nces.ed.gov/ipeds/>

longer to fill than other IT jobs, and they pay 16% more. That works out to a salary premium of \$12,700 per year.

- Yet for most IT workers, cybersecurity is one among many responsibilities rather than a dedicated role. More than half of jobs demanding cybersecurity skills are in fact other IT roles, where security is only one part of a broader job description as compared to jobs like Information Security Analyst, where security is their primary function.
- For each cybersecurity opening, there was a pool of only 2.3 employed cybersecurity workers for employers to recruit. That is almost exactly the same ratio of openings-to-employed workers as in 2015-16. By comparison, there are 5.8 employed workers per job opening across the economy in general. Even with the expansion of cybersecurity programs, supply has not kept up with demand.
- The industry is increasingly turning to automation for solutions. Demand for automation skills in cybersecurity roles

has risen 255% since 2013 and demand for risk management rose 133%.

- Public cloud security (170%) and knowledge of the Internet of Things (140%) are projected to be the fastest-growing skills in cybersecurity over the next five years.

The cybersecurity challenge shows no sign of slowing, either for government or business. As we write this, major functions of the Baltimore city government are held hostage by a ransomware attack,² while the Federal Election Commission has approved a nonpartisan group's effort to provide free cybersecurity support to presidential campaigns.³ The U.S. intelligence community reported in January 2019 that all four of America's main global military adversaries (Russia, China, North Korea, and Iran) are investing in cyberwarfare.⁴ A report from Cisco found that half of all cyberattacks cost businesses in excess of \$500,000 per incident.⁵ The increasing and ever-changing cybersecurity problem challenges employers both to train more aggressively and to sharpen their talent strategies to find the skilled defenders they need.

2 The New York Times, "Hackers Are Holding Baltimore Hostage: How They Struck and What's Next," May 22, 2019, <https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html>

3 Federal Election Commission, "FEC approves advisory opinion, discusses AO request and draft interpretive rule," May 23, 2019, <https://www.fec.gov/updates/fec-approves-advisory-opinion-discusses-ao-request-and-draft-interpretive-rule/>

4 Senate Select Committee on Intelligence, "Worldwide Threat Assessment of the U.S. Intelligence Community," Jan. 29, 2019, <https://www.intelligence.senate.gov/sites/default/files/documents/os-dcoats-012919.pdf>

5 Cisco, "Cisco 2018 Annual Cybersecurity Report," accessed Jan. 20, 2019; <https://www.cisco.com/c/en/us/products/security/security-reports.html>

Methodology: Defining the Cybersecurity Jobs Landscape

Historically, one of the barriers to building the cybersecurity workforce was finding comprehensive information on the size and scope of demand for cybersecurity workers. To overcome this challenge and quantify a broader swath of the cybersecurity job market, Burning Glass turned to its database of over 150 million unique online job postings. Burning Glass built a definition of the cybersecurity job market that includes all job openings with cybersecurity-related job titles, skills, or certifications. This enables a more comprehensive and granular view of the cybersecurity jobs landscape.



2.

Findings

A Tight Cybersecurity Job Market Continues

Cybersecurity has made a definitive mark on the broader IT workforce. From September 2017 through August 2018, there were 313,735 cybersecurity job openings across the United States, accounting for 13% of all IT jobs. Demand for these roles has grown at a rapid pace, increasing 94% since 2013. By comparison, demand for all IT jobs grew only 30% during the same period. That means demand for cybersecurity workers grew three times faster than IT jobs overall.

As demand for cybersecurity workers has boomed, the supply of these workers has struggled to keep pace, notwithstanding a significant influx of new talent into the field. Training new workers is important, but the vast majority of jobs are filled by people already in the workforce. This is true both in and out of cybersecurity. So the number of currently employed workers to posted job openings is a key indicator of how tight the job market is at a given moment. When the number is low, it means employers have fewer opportunities to “poach” cybersecurity workers from other companies and must look to other tactics—cyber training for current workers, or attracting new talent, for example—to fill their needs for cybersecurity professionals.

When we looked at the cybersecurity market in 2015, we found employers had 2.2 employed workers to recruit from for every cybersecurity opening. In 2017-18, there were 2.3, at best a minor improvement. By contrast, employers had five workers to recruit from for every opening in 2015-16, increasing to 5.8 in 2017-18 as unemployment fell overall and more individuals entered the workforce.

Cybersecurity roles take 20% longer to fill than other IT jobs.

Another sign of a tight market is how long it takes to fill a job. Cybersecurity is just one specialty in the information technology world, accounting for 13% of all IT job openings. On average, IT jobs take 41 days to fill. Cybersecurity roles, however, take 20% longer to fill (50 days) suggesting they are considerably more difficult to fill than other IT jobs, which are already among the hardest-to-fill jobs in the market. This tight hiring market is driving up salaries, and the average advertised salary for a cybersecurity job is now \$93,540—16% more than the average for all IT jobs. This translates to an average salary premium of more than \$12,700 per year.

A Responsibility More than a Role

Cybersecurity is a specialty, but most of the workers who practice it are not specialists. In many organizations, cybersecurity is a task built into other IT jobs, such as network administrators. Overall, these “cyber-enabled” jobs form the majority (56%) of all cybersecurity-related openings.

But the full-time cybersecurity specialists command higher salaries. On average, a core cybersecurity position pays over \$9,000 per year more than a cyber-enabled position. This is driven by an even more severe lack of talent among core cybersecurity roles than the broader

cybersecurity market: The ratio of workers-to-openings is 1.5 employed workers per opening for core cybersecurity workers, compared to 3.4 employed workers for every cyber-enabled opening.

Not surprisingly, given their broader responsibilities, cyber-enabled positions demand more general IT and business skills, such as project management, network engineering, SQL, system administration, and technical support. Core cybersecurity roles have a greater demand for skillsets and tools directly related to information security, such as information systems, cryptography, information assurance, network scanners, and security operations.

Key Skills: Core Cyber Jobs vs. Cyber-Enabled Jobs

Core Cyber	Cyber-Enabled
Information Security	Information Security
Information Systems	Network Security
Network Security	Project Management
LINUX	Information Systems
Project Management	LINUX
Cryptography	Customer Service
Vulnerability Assessment	Cisco
UNIX	System Administration
Information Assurance	SQL
Python	Technical Support

The Clogged Cyber Pipeline: Demand for Education, Experience, and Certifications

Most cybersecurity employers aren't looking for newbies, and they aren't looking for those without a college degree, either. Some 88% of cybersecurity postings specify a bachelor's degree or higher, and roughly the same percent demand at least three years of experience.

High education and experience requirements make skills gaps harder to close. Because cybersecurity jobs require years of training and relevant experience, skills gaps cannot easily be resolved through short-term

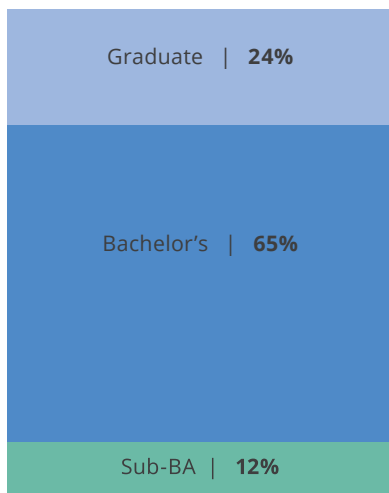
solutions. This also creates a chicken-and-egg problem: If there are few opportunities for workers to enter the cybersecurity field, there are few opportunities to build the next generation of cybersecurity workers.

Therefore, employers and training providers must work together to cultivate a talent pipeline for these critical roles.

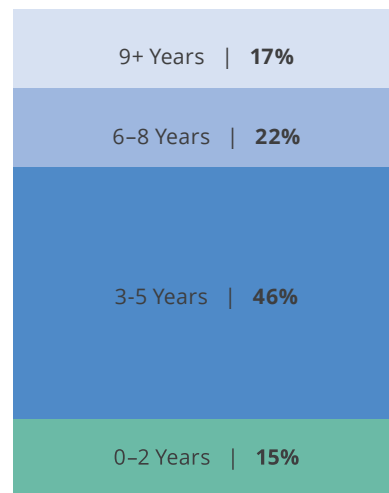
Yet at the same time, cybersecurity is largely defined by certifications. Nearly six in 10 (59%) of all cybersecurity positions request at least one certification. By comparison, only 20% of overall advertised IT jobs request an industry certification. These credentials offer stackable credentials for workers to enter and advance in cybersecurity.⁶ Entry-level workers, for example, can obtain foundational

Cybersecurity education and experience requirements

Cybersecurity education requirements



Cybersecurity experience requirements



6 For detailed career pathways in cybersecurity, visit the website Burning Glass Technologies developed in partnership with CompTIA and the National Initiative for Cybersecurity Education: Cyberseek.org.

certifications such as Security+, which represents an entry point into the field and is by far the largest cybersecurity certification in terms of total holders. Experienced workers can target more advanced certifications such as CISSP, which requires holders to pass a rigorous exam and possess at least five years of information security experience—common requirements among advanced certifications.

However, many of these certifications have as many annual job openings as certification holders—and in some cases openings eclipse certification holders,

Managing Risks, Embracing Robots

The skills employers are demanding in cybersecurity roles signal a broader strategic shift. A key element of cybersecurity work has been compliance: ensuring that best practices—or in many cases, government regulations or security controls—are followed across the organization. Certainly, compliance failures have played a role in many breaches: unsecure passwords, lost laptops, and failure to follow procedures that compartmentalize information within an organization. Moreover, federal law plays an important role in health care privacy (via the HIPPA law) and finance (Sarbanes-Oxley).

The skills employers are demanding in cybersecurity roles signal a broader strategic shift.

such as for CISSP, CISA, and CISM—which underscores the hiring difficulty for roles requesting these certifications. The relative dearth of workers with these certifications suggests that employers may need to rethink their requirements and determine which credentials are essential or just desirable. To expand their candidate pool and reduce their hiring difficulty, employers should consider removing nonessential credentials from their requirements.

Nonetheless, many of the most prominent breaches occurred at organizations with strict adherence to security frameworks and controls. In response, many cybersecurity experts are now advocating a different approach, focused on managing risk. Given that there is a greater threat from professional hackers or even governments who probe networks repeatedly for weaknesses over time, a risk-based approach offers more flexibility and faster responses than a rigid focus on following rules.

High-Demand Skills in Key Cybersecurity Fields

Risk	Automation
Risk Management	Python
Risk Assessment	PERL
Internal Auditing	JAVA
COBIT	Splunk
Risk Management Frameworks (e.g. NIST)	Microsoft PowerShell
Information Assurance	C++
Audit Planning	Ruby
External Auditing	Bash

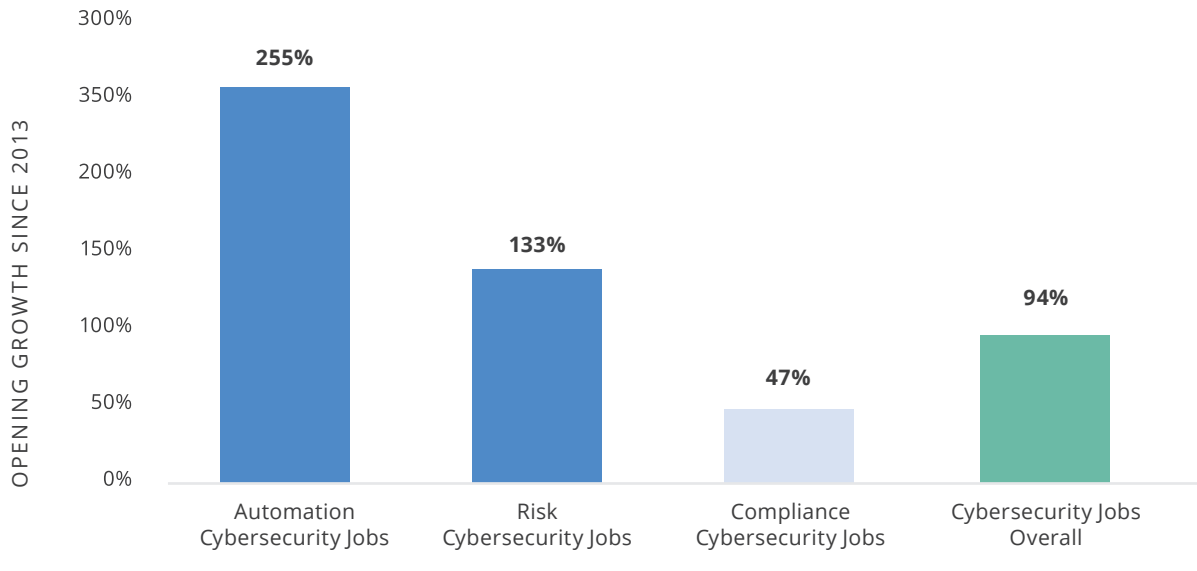
In cybersecurity job postings, skills associated with managing risk have risen 133% since 2013. The shift is particularly pronounced in finance: The industry accounts for 31% of all risk-related cybersecurity demand, despite accounting for only 18% of overall cybersecurity demand.

By contrast, demand for compliance skills rose more slowly than risk management, and lags behind growth in the cybersecurity job market overall. It's possible that in some cases compliance skills are considered so basic that employers don't believe they need to mention them in job descriptions, but there's no doubt that a cybersecurity worker

who understands risk management is in greater demand.

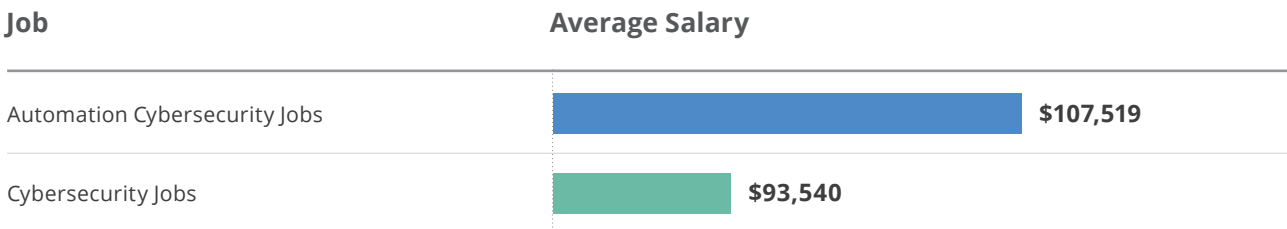
What's true of risk management is even truer of automation. Cybersecurity experts have argued that the shortage of trained workers and the rapid pace of technology makes automation and artificial intelligence viable options to protect the virtual barricades, and demand for automation-related skills within cybersecurity jobs spiked 255% since 2013. In addition, as more and more products become interconnected via the Internet of Things, understanding the growing automation of tasks is crucial to guarding them from attack.

Growth for Automation, Risk, and Compliance Skills in Cybersecurity since 2013



Cybersecurity jobs with an automation component also pay considerably more, carrying what amounts to a nearly \$14,000 average annual salary premium over other roles. Therefore, organizations considering hiring cybersecurity workers with automation-related skills will need to balance the increased payroll costs against the potential efficiencies gained through process automation.

Average Salary: Automation Jobs in Cybersecurity vs. All Cybersecurity Jobs



Different Companies, Different Demands

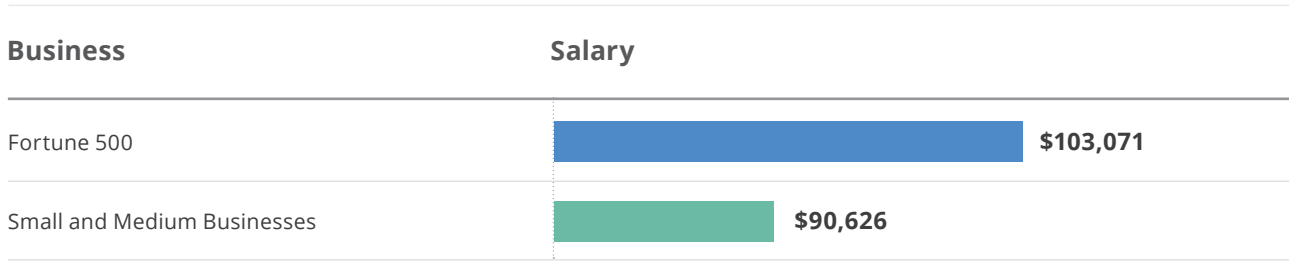
Cybersecurity is not a one-size-fits-all field: To be effective, you need to understand the industry you are protecting. The demand for cybersecurity skills varies by industry, and so do the precise skills needed.

Professional Services, Finance, and Manufacturing and Defense are the leading sectors for cybersecurity professionals. However, the sectors showing the fastest increases in demand for cybersecurity workers are Finance and Public Administration—arguably the two sectors facing the most persistent and sophisticated threats.

Cybersecurity Openings Share and Growth by Industry Sector

Industry Sector	Share of Cybersecurity Openings	Openings Growth: 2013 to Sept 2017–Aug 2018
Professional Services	41%	91%
Finance and Insurance	18%	139%
Manufacturing and Defense	10%	21%
Information	7%	44%
Public Administration	5%	138%
Educational Services	4%	43%
Administrative and Waste Services	3%	36%
Health Care and Social Assistance	3%	36%
Retail Trade	2%	51%
Other	6%	101%

Average Cybersecurity Salary: Fortune 500 vs Small and Medium Businesses



Just as there are differences in the cyber workforce between industries, there are differences in the cyber workforce between firms of different sizes. One of the most critical differences is the salary gap between large and small firms. All kinds of businesses have cybersecurity needs, but bigger companies have a definite advantage in bidding wars for talent. Burning Glass’ analysis of posted salary data shows that Fortune 500 companies can—and do—pay more than small- and medium-sized businesses.⁷ Small- and medium-sized businesses are

already attractive targets for cybercriminals, and their disadvantage in the market for cybersecurity talent exacerbates their challenges protecting their digital assets.

Into the Cloud: Projected Demand for Cybersecurity Skills

Cybersecurity threats keep evolving, particularly as more and more technology becomes digitally connected. The Internet of Things—“smart” appliances, houses, and other everyday technology—is bringing both

⁷ Small- and medium-sized businesses are defined as those with no more than 100 annual openings.

Projected Demand for Cybersecurity Skills

Skill	2018 Openings	2018–2023 5-Year Projected Growth
Public Cloud Security	1,333	170%
IoT Network Security	1,092	144%
Cybersecurity Strategy	3,184	120%
Dynamic Application Security Testing	1,892	120%
Cloud Security Architecture	1,902	113%
NIST Cybersecurity Framework	19,508	111%
Cybersecurity Assessments	9,543	93%
Cloud Security Applications	1,148	87%
Salesforce Security	2,300	77%
Open Web Application Security Project (OWASP)	10,410	61%

more opportunities and vulnerabilities for cybercriminals to attack. In addition, the move toward storing data and working “in the cloud” as opposed to on-site servers will also change the skills in demand. Spending on the Internet of Things, for example, is projected to reach \$3 trillion by 2026.⁸

Burning Glass projections show both of these skillsets will see the fastest increases in demand over the next five years. In addition, demand for broader skills, such as cybersecurity strategy and knowledge of the NIST Cybersecurity Framework,⁹ will increase much more quickly than the market overall.

⁸ Business Insider, “IoT Report: How Internet of Things technology growth is reaching mainstream companies and consumers,” Jan. 28, 2019, www.businessinsider.com/internet-of-things-report

⁹ For more about the NIST Cybersecurity Framework, visit www.nist.gov/cyberframework

3.

Implications

The cybersecurity talent pipeline has not kept up with demand for years—if it ever did. The growing dependence on the Internet in the economy, and in daily life, ensures the demand for cybersecurity talent will continue to grow. Therefore, firms, training providers, and workforce development officials must develop strategies and tactics to manage the talent shortage. Below we present three options informed by this research.

Build, rather than buy, cyber talent

Nearly six in 10 jobs demanding cybersecurity skills are “cyber-enabled,” meaning cybersecurity is one part of a broader set of responsibilities for many workers. While this raises a number of issues from a management perspective (such as whether cyber defense is enough of a priority in some organizations and roles), it also offers an opportunity. Workers in these jobs can be trained up or moved over from similar roles with additional training. Essentially, this would focus on getting these workers over the “last mile” of skills and into cyber-enabled jobs. This expands the potential pool of talent to the entire IT industry, in addition to building the infrastructure to allow security to be built in throughout the IT process.

Focus on credentials in short supply

Certifications are crucial in the cybersecurity field, and yet there are far more jobs available than there are certified workers. To be sure, many employers may benefit from removing certification requirements—there are always a handful of openings requesting two years of experience along with credentials that

can only be attained with at least five years of experience—but certifications are nonetheless important and undersupplied signaling mechanisms in the cybersecurity job market. And the biggest gaps seem to be at the top of the pyramid. At the very apex, the Certified Information Systems Security Professional, there is fewer than one certification holder per opening. Other advanced certifications, such as Certified Information Systems Auditor and Certified Information Systems Manager, also suffer from serious shortfalls in talent.

Of course, you cannot get workers into advanced certificate programs until they master the basics. IT recruitment programs can help bring more people into entry-level certifications such as Security+, alternative pathways can draw from different labor pools, and more effort needs to be made to reach out to a broader, more diverse population. But more effort also needs to be put into helping workers advance.

Promote return on investment for workers

Many existing workers possess the skills required to enter or advance in a career in cybersecurity, and they just need to develop the “last mile” skills necessary to make the transition. Therefore, working learners

present a strong opportunity to bring new blood into the cybersecurity workforce. A different set of incentives will be needed for working learners to invest in advanced training, however. One of the crucial issues for any working learner is whether getting additional training will pay off, considering the investment of time and money. Working learners—the prime candidates for advanced certifications like CISSP, CISM, and CISA—not only have to come up with the money to pay for training, but also juggle demands of family and their current job.

This is an area where employers have many tools to encourage advanced training. In addition to tuition reimbursement and other educational benefits, employers can also offer flex time and other accommodations to workers attending additional courses.

Most importantly of all, employers can be clear on what the payoff will actually be in terms of increased salary and career advancement. For example, the advanced CISSP credential carries an average salary premium of \$26,000 over entry-level credentials. Showing the salary premiums available in a specific company, along with clear career pathways, could persuade more workers that gaining additional qualifications is worth the effort.

4.

Appendix

Job Openings by NICE Cybersecurity Workforce Framework Category

Below are cybersecurity job postings from September 2017 to August 2018 broken down by the categories of the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework (NICE Framework). This framework, published by the National Institute of Standards and Technology, is a national taxonomy and common lexicon to describe cybersecurity work, and workers, regardless of where, or for whom, the work is performed. More details are available at Cyberseek.org.

NICE Workforce Category	Job Openings Sept 2017–Aug 2018	Description
Operate and Maintain	207,190	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Securely Provision	186,864	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.
Protect and Defend	129,716	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
Analyze	124,389	Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Oversee and Govern	88,175	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Collect and Operate	49,825	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Investigate	3,496	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

5.

Resources & Acknowledgments

Cyberseek.org:

A joint resource of Burning Glass Technologies, CompTIA, and the National Institute for Cybersecurity Education, CyberSeek provides detailed, actionable data about supply and demand in the cybersecurity job market.

National Initiative for Cybersecurity Education (NICE):

www.nist.gov/itl/applied-cybersecurity/nice

CompTIA

www.comptia.org

GIAC

www.giac.org

ISACA:

www.isaca.org

ISC²:

www.isc2.org

International Association of Privacy Professionals:

www.iapp.org

Authors

Written by Will Markow, Scott Bittle, and Pang-Cheng Liu. Special thanks to Matt Sigelman and Dan Restuccia.

About Burning Glass

Burning Glass Technologies delivers job market analytics that empower employers, workers, and educators to make data-driven decisions. The company's artificial intelligence technology analyzes hundreds of millions of job postings and real-life career transitions to provide insight into labor market patterns. This real-time strategic intelligence offers crucial insights, such as which jobs are most in demand, the specific skills employers need, and the career directions that offer the highest potential for workers. Find out more at burning-glass.com.

Photo Credits

Page 2: Photo courtesy of U.S. Navy/ PO2 William Sykes

Page 26: Photo courtesy of the Federal Bureau of Investigation

Burning Glass Technologies

One Lewis Wharf

Boston, MA 02110

+1 (617) 227-4800

www.burning-glass.com

