burningglass®
CAREERS IN FOCUS

Job Market Intelligence: Cybersecurity Jobs, 2015

Introduction: Cybersecurity and the Job Market

American employers have realized the vital importance of cybersecurity—but that realization has created a near-term shortage of workers that may require long-term solutions.

Cybersecurity was once the province of defense contractors and government agencies, but in this, the third edition of our annual analysis, we find **hiring has boomed in industries like Finance, Health Care, and Retail**. A glance at the headlines is enough to explain why. In addition to the federal Office of Personnel Management, recent cyber breaches have hit major consumer companies like Chase and Target. According to PwC's 2015 State of US Cybercrime Survey, a record 79% of survey respondents said they detected a security incident in the past 12 months. Many incidents go undetected, however, so the real tally is probably much higher.

Yet we are also seeing multiple signs that demand for these workers is outstripping supply. **Job postings for cybersecurity openings have grown three times as fast as openings for IT jobs overall** and it takes companies longer to fill cybersecurity positions than other IT jobs. That's bad for employers but good news for **cybersecurity workers, who can command an average salary premium of nearly $6,500 per year**, or 9% more than other IT workers.

Or put another way, there were nearly 50,000 postings for workers with a CISSP certification in 2014, the primary credential in cybersecurity work. That amounts to three-quarters of all the people who hold that certification in the United States—and presumably most of them already have jobs.

This is a gap that will take time to fill. The skills for some IT positions can be acquired with relatively little training, but cybersecurity isn't one of them. For example, five years of experience are required to even apply for a CISSP certification. That doesn't even consider the rising demand for experience in a specific industry, like finance or health care. This suggests that the shortage of cybersecurity workers is likely to persist, at least until the education and training system catches up.

Key Trends in Cybersecurity Demand

Cybersecurity jobs are in demand and growing across the economy

- The Professional Services, Finance, and Manufacturing/Defense sectors have the highest demand for cybersecurity jobs.
- The fastest increases in demand for cybersecurity workers are in industries managing increasing volumes of consumer data such as Finance (+137% over the last five years), Health Care (+121%), and Retail Trade (+89%).

Positions calling for financial skills or a security clearance are even harder to fill than other cybersecurity jobs

- The hardest-to-fill cybersecurity jobs call for financial skills, such as Accounting or knowledge of regulations associated with the Sarbanes-Oxley Act, alongside traditional networking and IT security skills. Because finance and IT skills are rarely trained for together, there is a skills gap for workers who meet the requirements of these "hybrid jobs."
- More than 10% of cybersecurity job postings advertise a security clearance requirement. These jobs, on average, take 10% longer to fill than cybersecurity jobs without a security clearance.

Cybersecurity positions are more likely to require certifications than other IT jobs

- One third (35%) of cybersecurity jobs call for an industry certification, compared to 23% of IT jobs overall.

Cybersecurity employers demand a highly educated, highly experienced workforce

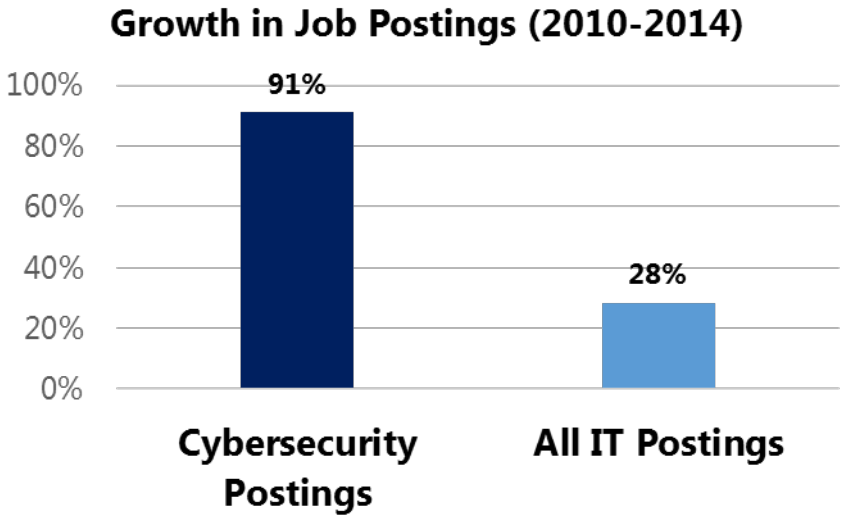
- Some 84% of cybersecurity postings specify at least a bachelor's degree, and 83% require at least three years of experience. Because of the high education and experience requirements for these roles, skills gaps cannot easily be resolved though short-term solutions. Employers and training providers must work together to cultivate a talent pipeline for these critical roles.

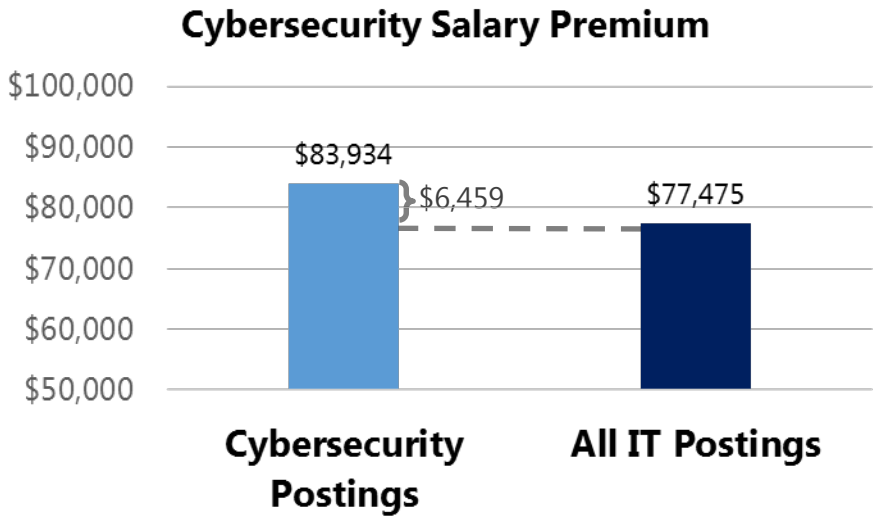
Geographically, cybersecurity jobs are concentrated in government and defense hubs, but are growing most quickly in secondary markets

- On a per capita basis, the leading states are Washington D.C., Virginia, Maryland, and Colorado; all have high concentrations of jobs in the federal government and related contractors.

By the Numbers: The Cybersecurity Job Market

- In 2014, there were 238,158 postings for cybersecurity-related jobs nationally. **Cybersecurity jobs account for 11% of all IT jobs.**
- Cybersecurity postings have **grown 91%** from 2010-2014. This growth rate is more than faster than IT jobs generally.
- Cybersecurity posting advertise a 9% salary premium over IT jobs overall.
- Cybersecurity job postings took **8% longer to fill than IT job postings overall.**
- The demand for certificated cybersecurity talent is outstripping supply. In the U.S., employers posted 49,493 jobs requesting a CISSP, recruiting from a pool of only 65,362 CISSP holders nationwide.*





*According to the International Information System Security Certification Consortium, Inc., (ISC)²® membership counts as of July 14, 2015

Cybersecurity Demand Grows in Finance, Professional Services

- **Professional Services, Finance, and Manufacturing & Defense are the leading sectors** for cybersecurity professionals.
- Sectors managing increasing volumes of consumer data such as **Finance, Health Care, and Retail Trade have the fastest increases in demand** for cybersecurity workers.
- Within these sectors, demand for cybersecurity professionals is growing rapidly in more specific industry subsectors not typically associated with cybersecurity, including Air Transportation (+221%) and Accommodation (+157%).

Industry Sector	% of Cybersecurity Postings	Number of Cybersecurity Postings (2014)	2010 - 2014 Posting Growth
Professional Services	37%	49,765	57%
Finance and Insurance	13%	17,873	131%
Manufacturing & Defense*	12%	15,968	57%
Public Administration	7%	9,725	N/A**
Information	6%	8,522	65%
Health Care and Social Assistance	6%	7,915	118%
Retail Trade	3%	3,505	120%
Other	15%	19,983	N/A**

*The Manufacturing Sector includes services divisions of a number of defense contractors (e.g. Raytheon) and computer manufacturers (e.g. Hewlett Packard).
** Industry growth rates are suppressed for the Public Administration and Other industry sectors because a significant portion of labor market demand in these industries exists offline.

Engineers, Managers, and Analysts Dominate the Field

The cybersecurity workforce covers a range of job types and skills. This includes advanced Engineer and Architect roles, Auditors (which are concentrated in Finance) and Specialists, which typically have lower entry level requirements.

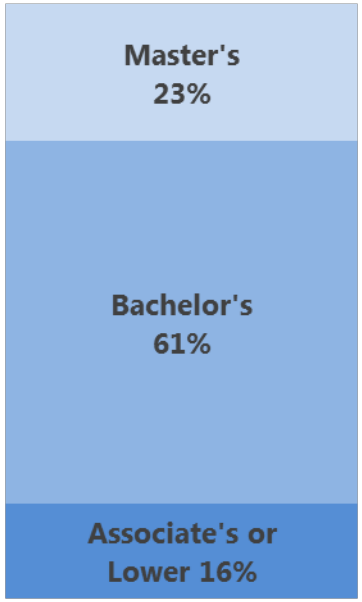
Title	% of Cybersecurity Postings	Number of Cybersecurity Postings (2014)
Engineer (e.g. Security Engineer, Information Assurance Engineer)	26%	42,355
Manager/Admin (e.g. Data Security Administrator, Information Security Manager)	19%	30,586
Analyst (e.g. IT Security Analyst, Cyber Intelligence Analyst)	18%	28,853
Specialist/Technician (e.g. IT Security Specialist, Infosec Technician)	10%	15,289
Architect (e.g. Security and Privacy Architect, Network Security Architect)	5%	8,409
Auditor (e.g. IT Auditor)	5%	7,533
Consultant (e.g. Network Security Consultant, Infrastructure Security Consultant)	4%	6,294

Employers Demand More Education, Experience

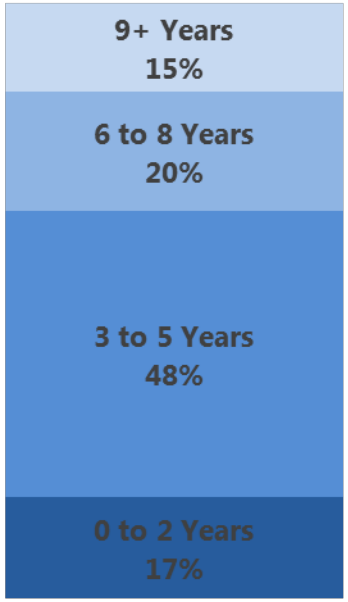
Cybersecurity jobs require significant education and experience. Some 84% of cybersecurity postings specify at least a bachelor's degree, and just as many (83%) require at least 3 years of experience, with an average of 5.4 years.

High education and experience requirements make skills gaps hard to close. Because cybersecurity jobs require years of training and relevant experience, skills gaps cannot easily be resolved though short-term solutions. Employers and training providers must work together to cultivate a talent pipeline for these critical roles.

Requested Education Level*



Minimum Experience



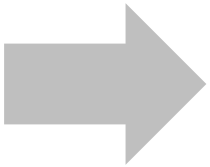
Certification Shapes the Path to Advancement

The cybersecurity job market is shaped by certifications, and job seekers of all experience levels can improve their employment opportunities by obtaining the relevant credentials. Entry-level workers, for example, can obtain foundational 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.

Entry-Level Certifications

Typically require less than 3 years of experience

- Security+
- GIAC Security Essentials (GSEC)
- Certified Information Privacy Professional (CIPP)
- Systems Security Certified Practitioner (SSCP)



Advanced Certifications

Typically require at least 3-5 years of experience

- Certified Information Systems Security Professional (CISSP)*
- Certified Information Systems Auditor (CISA)*
- Certified Information Security Manager (CISM)*
- GIAC Certified Incident Handler (GCIH)
- GIAC Certified Intrusion Analyst (GCIA)

*Requires a minimum of 5 years of information security experience.

Certification is More Common in Cybersecurity Jobs

Cybersecurity jobs are highly certificated: More than one in three (35%) of all cybersecurity positions request at least one of the certifications listed below. Only 23% of overall advertised IT jobs request an industry certification.

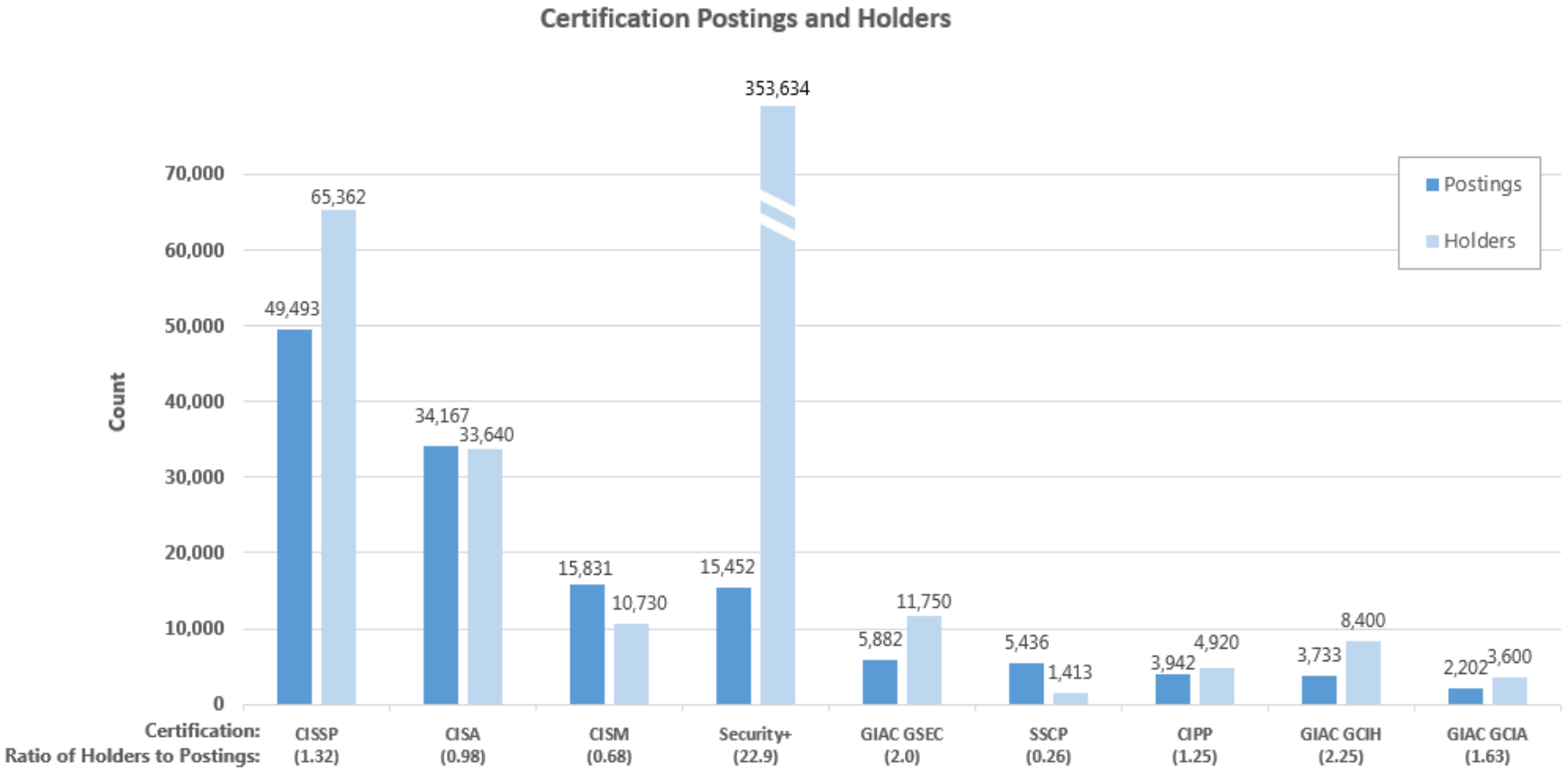
Certification increases salary: Security+ represents the entry-level certification for cybersecurity roles, and postings requesting it advertise an average salary of $75,484. This serves as a baseline salary for certified cybersecurity workers, and as workers obtain additional certification they can qualify for ever greater salaries. Postings requesting CISSP, for example, advertised an average salary of $93,010 – a premium of $17,526 over the average salary for Security+.

Certification*	% of All Cybersecurity Postings	Number of Cybersecurity Postings (2014)	Average Salary with Certification	Premium Over Security+ Average Salary
CISSP Certified Information Security Professional	21%	49,493	$93,010	$17,526
CISA Certified Information Systems Auditor	14%	34,167	$86,238	$10,754
CISM Certified Information Security Manager	7%	15,831	$95,450	$19,966
Security+ Systems Security Certified Practitioner	6%	15,452	$75,484	$0
GIAC GSEC GIAC Security Essentials	2%	5,882	$81,631	$6,147
SSCP Systems Security Certified Practitioner	2%	5,436	$80,718	$5,234
CIPP Certified Information Privacy Professional	2%	3,942	$90,550	$15,066
GIAC GCIH GIAC Certified Incident Handler	2%	3,733	$92,759	$17,275
GIAC GCIA GIAC Certified Intrusion Analyst	1%	2,202	$84,392	$8,908

*Certification Requirements are not mutually exclusive

Certifications: Too Many Openings Chasing Too Few Workers

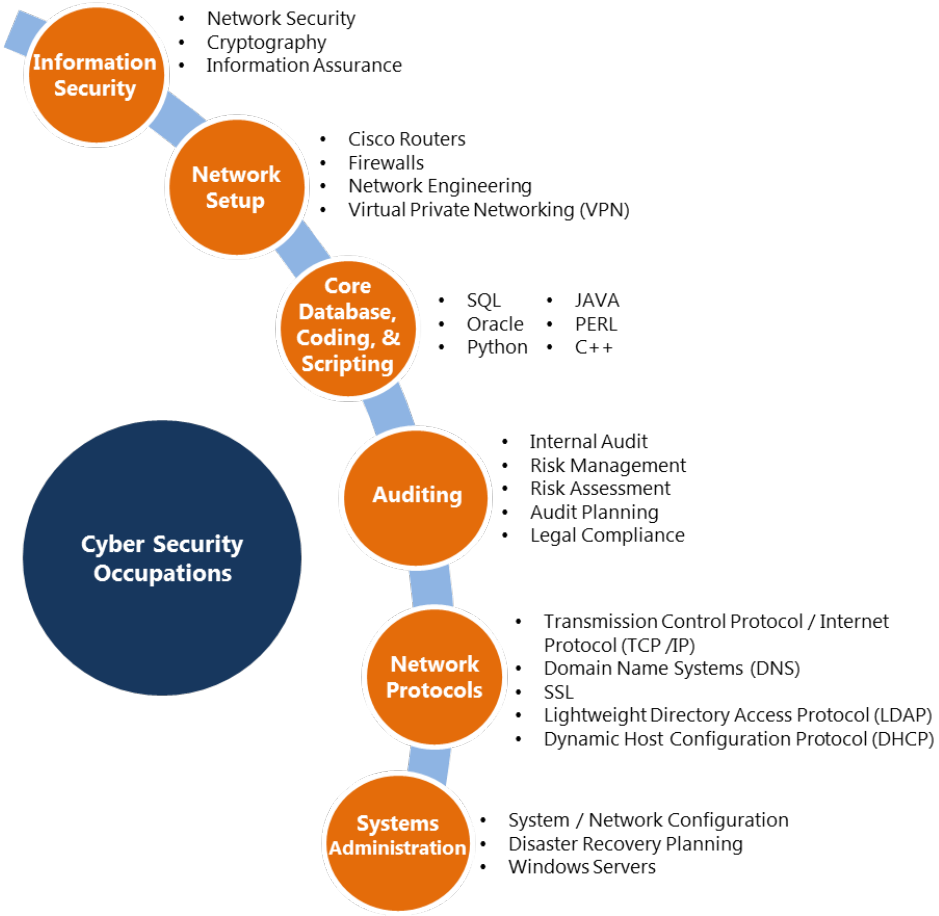
Employers prefer workers with cybersecurity certifications, but there can be three or more postings for every certificate holder. When you consider that most of these certificate holders are already employed, the situation looks even better for workers. Even the generous supply of Security + holders is somewhat misleading. Security + is a entry level certificate, so many people with more advanced credentials have one, and the openings that require it are relatively low-level.



Note: Different certifying organizations report slightly different counts of holders. For example, some may report total certifications awarded, while others may report only active certification holders.

Cybersecurity Workers Need to Know IT and Their Industry

The graphic below describes the expertise required for various cybersecurity roles in demand. On top of those skills, job postings often call for additional knowledge in certain information-sensitive industries, such as Health Care; Finance; and Manufacturing and Defense.



Additional Skill and Domain Knowledge Requirements by Industry

Health Care:

Skills:
- Generally Accepted Accounting Principles
- Financial Reporting

Compliance & Standards:
- HIPAA
- HITECH
- Payment Card Industry Data Security Standard (PCI DSS)

Finance & Accounting:

Skills:
- Generally Accepted Accounting Principles
- Financial Reporting

Compliance & Standards:
- Payment Card Industry Data Security Standard (PCI DSS)
- Sarbanes-Oxley Act (SOX)

Manufacturing & Defense:

Compliance & Standards
- JAFAN 6/9 & 6/3, DCID 6/3 and DIACAP
- NERC Reliability Standards

Hybrid Jobs Combining Different Skills are Hardest to Fill

Employers often struggle to fill positions with specialized skill requirements. The fastest-growing skills include industry knowledge areas, such as HIPAA requirements in Health Care and Risk Management, and Accounting in Finance. The hardest-to-fill skills are typically related to finance, such as Information Assurance, Sarbanes-Oxley, and Accounting. **Finding candidates with these unique skill sets can take roughly 17% longer to fill on average than other cybersecurity job openings**.

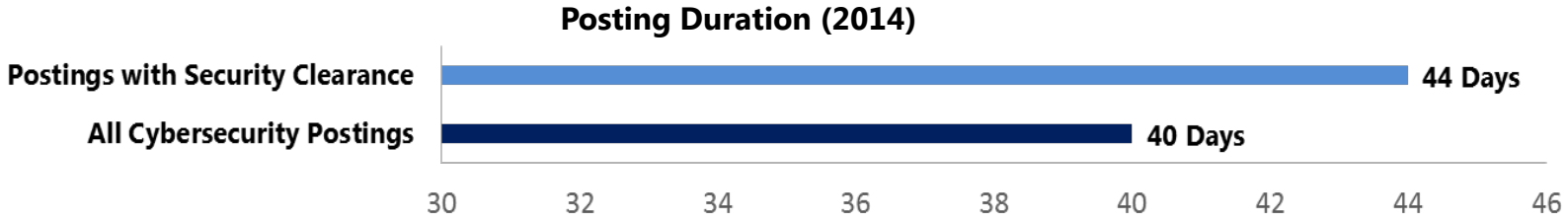
The difficulties in filling jobs that require a combination of IT security and financial skills reflects a broader trend in the market: hybrid jobs which combine skill sets that are not traditionally trained for together. This often results in skills gaps where employers struggle to find employees that meet these skill needs.

Fastest-Growing Skills in Cybersecurity Job Postings	Five-Year Growth
Python	309%
HIPAA	248%
Risk Management	209%
Internal Auditing	200%
Audit Planning	170%
Risk Assessment	169%
ITIL	153%
Management Information Systems	132%
Accounting	121%
Configuration Management	106%

Hardest to Fill Skills in Cybersecurity Job Postings	Posting Duration	Time to Fill Above Average
Management Information Systems	50 days	+10 days
Information Assurance	47 days	+7 days
Sarbanes-Oxley	47 days	+7 days
Accounting	45 days	+5 days
Python	45 days	+5 days
Dynamic Host Configuration Protocol (DHCP)	45 days	+5 days
Configuration Management	44 days	+4 days
C++	44 days	+4 days
Public Accounting	43 days	+3 days
Internal Auditing	43 days	+3 days

Roles Requiring Security Clearance Take Longer to Fill

Workers with a security clearance—or the ability to get one—have an advantage. In 2014, there were 25,654 cybersecurity postings calling for a government Security Clearance to access classified information, representing 11% of all cybersecurity postings. On average, cybersecurity postings requesting Security Clearance remained open 10% longer than cybersecurity postings overall.



Average # of Days to Fill Online Job Postings in 2014

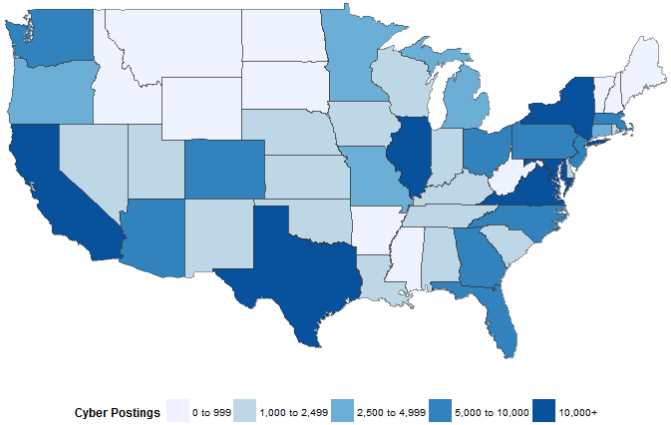
Industry Sector	Percentage of Industry Postings Requesting Security Clearance	Cybersecurity Postings Requesting Security Clearance (2014)
Public Administration	29%	2,793
Manufacturing & Defense*	19%	4,146
Professional Services	18%	10,317
Transportation and Warehousing	7%	107
Information	4%	471
Educational Services	4%	281
Finance and Insurance	2%	499
Healthcare and Social Assistance	1%	128

Cybersecurity Job Postings by State

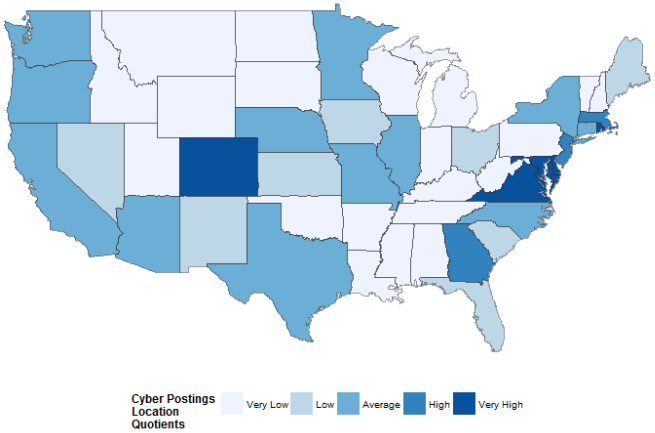
Top States by Total Postings*

	State	Total Postings	Location Quotient**	% Growth (2010-2014)
1	California	28,744	1.02	75%
2	Virginia	20,276	3.09	38%
3	Texas	18,525	0.92	113%
4	New York	14,089	0.97	104%
5	Illinois	11,428	1.16	163%
6	Maryland	11,406	2.40	39%
7	Florida	9,847	0.67	135%
8	Georgia	8,757	1.22	121%
9	New Jersey	8,268	1.21	80%
10	Massachusetts	7,911	1.45	92%
11	Colorado	7,688	1.77	111%
12	North Carolina	7,503	1.06	127%
13	Ohio	6,281	0.72	141%
14	Pennsylvania	5,745	0.59	69%
15	Arizona	5,502	1.18	87%

Cybersecurity Job Postings in 2014 By State



Cybersecurity Location Quotient in 2014



*See Appendix 1 for state-level data tables on total postings and postings growth.

**Location quotients show how concentrated demand is in a particular geography relative to employment in that area. National location quotient equals 1.0; an LQ of 1.2 indicates that demand is 20% more concentrated than nationally.

Cybersecurity Job Postings by City

Top Cities by Total Postings

	City (MSA)	Total Postings	% Growth (2010-2014)
1	Washington, D.C.	27,246	39%
2	New York	17,982	90%
3	San Francisco / San Jose	13,869	88%
4	Chicago	9,623	164%
5	Dallas	8,694	138%
6	Los Angeles	7,654	47%
7	Boston	6,918	99%
8	Atlanta	6,604	128%
9	Denver	4,744	176%
10	Baltimore	4,643	49%

Top Cities by Growth

	City (MSA)	Total Postings	% Growth (2010-2014)
1	Austin	2,937	209%
2	Columbus	1,916	178%
3	Denver	4,744	176%
4	Portland	2,424	175%
5	Chicago	9,623	164%
6	Miami	2,872	158%
7	Charlotte	3,000	147%
8	Tampa	2,606	145%
9	Dallas	8,694	138%
10	Atlanta	6,604	128%

Methodology

All jobs data in this report are drawn from Burning Glass's database of online job postings, which includes nearly 100M worldwide postings collected since 2007. Each day, Burning Glass visits close to 40,000 online jobs sites to collect postings. Using advanced text analytics, over 70 data fields are extracted from each posting including job title, occupation, employer, industry, required skills and credentials and salary. Postings are then deduplicated and placed in a database for further analysis.

This report classifies cybersecurity jobs as those which have a cybersecurity-related title, require a cybersecurity certification or request cybersecurity-specific skills. Cybersecurity-related titles used to define the roles analyzed in this report include "network security", "information security", "information assurance", and "penetration tester". Cybersecurity skills include information assurance, cryptography, computer forensics, malware analysis, 800-53, and ArcSight.

The data in this report use a broader definition of cybersecurity roles than Burning Glass's 2014 report examining the same topic. That report looked only at those roles with cybersecurity-specific titles, whereas this update includes jobs with cybersecurity titles, certifications or skills.

Appendix 1: State Data

	State	Total Postings	Location Quotient*	% Growth (2010-2014)
1	Alabama	2,159	0.66	31%
2	Alaska	556	1.00	17%
3	Arizona	5,502	1.18	87%
4	Arkansas	989	0.5	117%
5	California	28,744	1.02	75%
6	Colorado	7,688	1.77	111%
7	Connecticut	2,771	0.97	98%
8	Delaware	1,152	1.67	92%
9	Florida	9,847	0.67	135%
10	Georgia	8,757	1.22	121%
11	Hawaii	1,364	1.31	39%
12	Idaho	634	0.53	260%
13	Illinois	11,428	1.16	163%
14	Indiana	2,347	0.48	139%
15	Iowa	1,951	0.74	158%
16	Kansas	1,654	0.71	168%
17	Kentucky	1,753	0.58	209%
18	Louisiana	1,563	0.48	275%
19	Maine	791	0.74	214%
20	Maryland	11,406	2.40	39%
21	Massachusetts	7,911	1.45	92%
22	Michigan	4,225	0.59	117%
23	Minnesota	4,059	0.88	98%
24	Mississippi	827	0.45	161%
25	Missouri	4,004	0.86	88%

	State	Total Postings	Location Quotient*	% Growth (2010-2014)
26	Montana	344	0.43	189%
27	Nebraska	1,603	1.00	68%
28	Nevada	1,462	0.70	89%
29	New Hampshire	581	0.50	134%
30	New Jersey	8,268	1.21	80%
31	New Mexico	1,003	0.72	119%
32	New York	14,089	0.97	104%
33	North Carolina	7,503	1.06	127%
34	North Dakota	322	0.49	341%
35	Ohio	6,281	0.72	141%
36	Oklahoma	1,476	0.53	196%
37	Oregon	2,618	0.89	136%
38	Pennsylvania	5,745	0.59	69%
39	Rhode Island	1,267	1.53	134%
40	South Carolina	2,312	0.69	134%
41	South Dakota	354	0.50	195%
42	Tennessee	2,340	0.51	97%
43	Texas	18,525	0.92	113%
44	Utah	1,371	0.61	146%
45	Vermont	281	0.52	168%
46	Virginia	20,276	3.09	38%
47	Washington	5,119	0.96	94%
48	West Virginia	496	0.41	35%
49	Wisconsin	2,429	0.51	139%
50	Wyoming	176	0.37	245%

*Location quotients show how concentrated demand is in a particular geography relative to employment in that area. National location quotient equals 1.0; an LQ of 1.2 indicates that demand is 20% more concentrated than nationally.

Appendix 2: City (MSA) Data

	MSA	Total Postings	Location Quotient*	% Growth (2010-2014)
1	Atlanta	6,604	1.57	128%
2	Austin	2,937	1.88	209%
3	Baltimore	4,643	2.04	49%
4	Boston	6,918	1.52	99%
5	Charlotte	3,000	1.87	147%
6	Chicago	9,623	1.24	164%
7	Columbus	1,916	1.12	178%
8	Dallas	8,694	1.56	138%
9	Denver	4,744	2.03	176%
10	Detroit	2,753	0.84	112%
11	Houston	3,453	0.69	91%
12	Kansas City	1,884	1.06	111%
13	Los Angeles	7,654	0.78	47%
14	Miami	2,872	0.69	158%
15	Minneapolis	3,285	1.02	93%
16	New York	17,982	1.18	90%
17	Philadelphia	4,519	0.95	75%
18	Phoenix	4,044	1.26	101%
19	Portland, OR	2,424	1.30	175%
20	San Diego	3,068	1.32	94%
21	San Francisco / San Jose	13,869	4.89	88%
22	Seattle	4,105	1.32	100%
23	St. Louis	3,248	1.41	95%
24	Tampa	2,606	1.25	145%
25	Washington, D.C.	27,246	5.25	39%

*Location quotients show how concentrated demand is in a particular geography relative to employment in that area. National location quotient equals 1.0; an LQ of 1.2 indicates that demand is 20% more concentrated than nationally.

About Burning Glass

Burning Glass Technologies delivers job market analytics that empower employers, workers, and educators to make data-driven decisions. Burning Glass is reshaping how the job market works, with data that identify the skill gaps that keep job seekers and employers apart and tools that enable both sides to bridge that gap and connect more easily. 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.

Burning Glass' applications drive practical solutions and are used across the job market: by educators in aligning programs with the market, by employers and recruiters in filling positions more effectively, and by policy makers in shaping strategic workforce decisions. At the same time, Burning Glass' data-driven applications for workers and students help them choose career goals and build the skills they need to get ahead.

Based in Boston, Burning Glass is playing a growing role in informing the global conversation on education and the workforce, and in creating a job market that works for everyone.

For More Information

Dan Restuccia
Chief Analytics Officer
t +1 (617) 227-4800
drestuccia@burning-glass.com
www.burning-glass.com