Cybersecurity

Defending our Information Assets from an Ever Increasing Threat

---

Authored by

Burning Glass Technologies

BATEC National Center of Excellence in Computing and Information Technologies

Published

January 2016

UMASS BOSTON

This report was prepared with support from the National Science Foundation under grant DUE-110415 to the University of Massachusetts. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the editor and the principal investigators of the BATEC ATE Center. They do not necessarily reflect the views of the National Science Foundation.

FORWARD

There is a natural partnership between business and academia when it comes to workforce development.

- Corporate entities depend on a robust supply of qualified and capable workforce talent in order to grow their business and achieve their strategic objectives.
- Educational institutions have an implied contract with their students, promising them meaningful employment upon attainment of their degree credentials.

This partnership, though critically important, is particularly challenging in fields where the discipline is an emerging, tools, paradigms and best practices are still in development, and experience is relatively limited.

CyberSecurity is a new and emerging discipline that exhibits all of these characteristics. Moreover, it is a discipline which is critically important as the integrity and availability of our information infrastructure depends on it. Our computers, our databases and our networking platforms are under constant attack, and the stakes are quite high.

We've all been "hacked" at one time or another, and received some junk email, spam content, or annoying virus. We might categorize this experience as simply inconvenient and annoying. Corporate Cybercrime is, however, another matter. Strategic, intentional, and harmful attacks on corporate information resources can be costly, paralyzing and significant. World renowned experts forecast, without hesitation, that our next global conflict, "World War III", will be fought in Cyberspace.

This report, and the analysis contained herein, is both timely and valuable in its ability to enhance discussion, dialogue and collaboration between industry and academia about the emerging and pervasive discipline of CyberSecurity. This report analyzes the dimensions of the career pathway (number of jobs, average compensation, and geographical distribution of jobs) and the requirements of the employment opportunity (job responsibilities, technical and soft skill proficiencies).

It is our hope that this report will aid in the development of dynamic, innovative academic programs and a pipeline of workforce talent that support the industry needs for trained professionals. CyberSecurity is the hottest and most important discipline to take center stage in the next decade.

Lou Piazza

Lou Piazza
Director, BATEC

Contents

INTRODUCTION

The economic, privacy, and national security concerns stemming from rising cybersecurity threats are among the most critical issues facing the United States today. Cyber-related attacks have risen 38%[1], and all indicators suggest that the workforce needs in cybersecurity are a growing challenge for most employers as CyberSecurity job postings remain unfilled 21% longer than the most other jobs.

A workforce shortage in CyberSecurity talent has far reaching implications for our national, economic, and personal security. Mitigating this shortage will require coordination between a multitude of stakeholders, including employers, educators, and policymakers.

Some important initiatives are already underway – perhaps most notably, the National Initiative for Cybersecurity Education (NICE) has developed a framework to describe and profile the CyberSecurity workforce and improve Cyber literacy[2]. The Center for Academic Excellence (CAE) Initiative, jointly sponsored by the National Security Administration (NSA) and the Department of Homeland Security (DHS), is aimed at increasing access to the academic pathway in CyberSecurity.

This report, produced by Burning Glass Technologies and Broadening Advanced Technological Education Connections (BATEC), aims to facilitate dialog among the aforementioned stakeholders providing a data-driven analysis of employment opportunities across the cybersecurity jobs landscape. It documents the workforce need and maps it into a set of cybersecurity academic pathway, describing the opportunities for workers to enter and advance within the field.

The field of CyberSecurity features both great promise and significant challenge. It promises high-demand, high-growth, and high-paying careers for skilled professionals, while threatening grave consequences if the workforce needs are not rapidly and effectively addressed.

The field of CyberSecurity is pervasive, and our national, economic and personal security is only as strong as the weakest link, the most vulnerable component. The principles of secure programming, network administration, digital forensics and information assurance will, and should, find their way into every computer-related academic pathway, and every IT-related job description.

We know that the status quo is not adequate to address the future needs of our nation. We hope that you find the information contained within this report informative and actionable, and encourage you to review it, discuss it, and debate it with stakeholders in your local geographical area. The integrity and privacy of our digital assets depends upon in.

[1] The Global State of Information Security Survey 2016. PwC.

[2] National Cybersecurity Workforce Framework.

THE TOP TEN THINGS YOU NEED TO KNOW…

1. The field of CyberSecurity is pervasive. Cyber-related skills are finding their way into every job in Information Technology, Digital Networking, and Computer Programming.
2. The cybersecurity job landscape is large and growing, and offers strong employment opportunities across the economy. There were 238,158 online job postings, in 2014, for cybersecurity job postings in the United States. This represents a 91% increase in the four year period 2010 to 2014.
3. CyberSecurity job postings remain open longer (8% longer than IT jobs overall) suggesting that these jobs are harder to fill than IT jobs in general.
4. CyberSecurity jobs pay well. The average advertised salary for these jobs is almost $84,000 – well above the average for all IT roles.
5. Cybersecurity jobs break into seven key broad categories (listed in order of employer demand): Engineers, Managers, Analysts, Specialists, Architects, Auditors, and Consultants.
6. The strongest growth in job postings is for the entry level roles of Specialist, Analyst and Auditor. These positions work in operations and defend information resources on a day-by-day basis.
7. Workforce opportunities in cybersecurity exist for job seekers of all educational levels. Candidates, with appropriate skills but not a bachelor's degree, can enter the workforce in the Specialist category where 37% of the positions do not require a four-year degree. A career in CyberSecurity does, however, require a commitment to continued education as the majority of positions require a Bachelor's Degree and many high paying positions require a Master's Degree.
8. The career pathway in CyberSecurity has reasonable definition. The job categories of Specialist and Analyst provide entry level opportunities for candidates with modest skills. The job category of Engineer provides economic incentive for continued educational achievement and skill development. The job categories of Manager, Architect and/or Consultant are the highest paying opportunities and require advanced training, experience, and/or certification.
9. There is a career transition opportunity for returning veterans. Many corporate CyberSecurity roles require similar competencies to those required in the military, and require security clearances which veterans either have in their possession or have experience qualifying for.
10. The workforce challenge can be best addressed when employers, educators, and policymakers work together in close collaboration. A shared vision and mutual understanding of the requisite skills, academic credentials and industry certifications required of a qualified candidate can empower educators to properly prepare an entry level workforce.

APPROACH AND METHODOLOGY

Burning Glass drew from its detailed database of online employer demand, which includes over 90 million current and historical job postings, to conduct this analysis. Burning Glass surveys postings from approximately 40,000 online job sites, extracting from each posting top-line information such as title, employer and industry. Duplicate postings are systematically eliminated; unique job postings are further analyzed. An artificial intelligence engine then reads each job description identifying job titles, skills, qualifications, and certifications.

Job postings requesting core cybersecurity job titles (e.g. information security analyst), skills (e.g. cryptography), or certifications (e.g. CISSP), were extracted from this database of online employment demand. These postings form the basis of the cybersecurity definition used throughout the report, and are heretofore referred to as "the CyberSecurity jobs".

The Cybersecurity jobs were grouped into categories based upon functional similarities. These categories were analyzed and compared across multiple factors, including magnitude of demand, skill and certification requirements, required education and suggested experience to understand the key dynamics shaping the employment ecosystem. The average length of time that job postings remained open was also calculated in an attempt to assess the relative difficulty that employers experience in filling these positions.

The dimensions (number of jobs, 4 year growth, average salary, duration of posting, and workforce density) was measured, and reported, both nationally, and regionally (in each of the following Metropolitan Statistical Areas (MSAs):

Bay Area[3]	Miami	Southern Ohio[4]
Boston	New York City	Washington D.C.
Chicago		

Burning Glass also surveyed the contents of its resume database analyzing almost 60 million career transitions. This results of this survey were used to document how, and when, workers move from one job category to another, and which skills and credentials trigger the opportunity for career advancement.

An internal catalog of mappings between military and civilian occupations was used to assess the opportunity for returning veterans to enter cybersecurity workforce. These mappings use skill requirements and on-the-job duties to define functional equivalency between military and civilian occupations.

Unless otherwise noted, all data in this analysis pertains to the calendar year 2014.

[3] Bay Area includes the Metropolitan Statistical Areas (MSAs) of San Francisco and San Jose

[4] Southern Ohio includes the MSAs of Springfield, Dayton, Cincinnati and Columbus

DETAILED FINDINGS

The CyberSecurity job landscape is large and growing, and offers strong employment opportunities across the economy. There were 238,158 online job postings in 2014, representing an increase of 91% since 2010. This robust growth has helped to make cybersecurity jobs are harder to fill than the industry norm. On average, cybersecurity jobs remained open for 40 days in 2014 – 8% longer than IT jobs overall.

CyberSecurity jobs are among the highest paying IT-related jobs. The average advertised salary is almost $84,000 – well above the average for comparable non-Cyber related jobs.

The resulting pressure on employers to attract and retain top cyber talent has driven average advertised salaries up to almost $84,000 – well above the average for all IT roles.

Our analysis of the CyberSecurity online postings suggests a segmentation of seven job categories, which account for 90% of the cybersecurity job openings and form a career pathway that employers, educators and job seekers can follow in their discussion about and focus their efforts in development of the cybersecurity workforce.

The table on the following page lists these categories (sorted by employer demand) with a description and set of representative titles.

There has been strong growth for entry-level roles, specifically in the two categories of Specialist and Analyst. These individuals work on operational teams involved in the day-to-day defense of information assets. Job postings, in each of these categories grew by more than 95% growth during the four year period, 2010 to 2014.

The largest job category, in terms of overall demand, was in the category Engineer. These individuals build and maintain the IT infrastructure (computers, networks, storage systems). The four year growth in this category was robust at 55%, but much less than the 91% growth rate experienced broadly across all cybersecurity jobs.

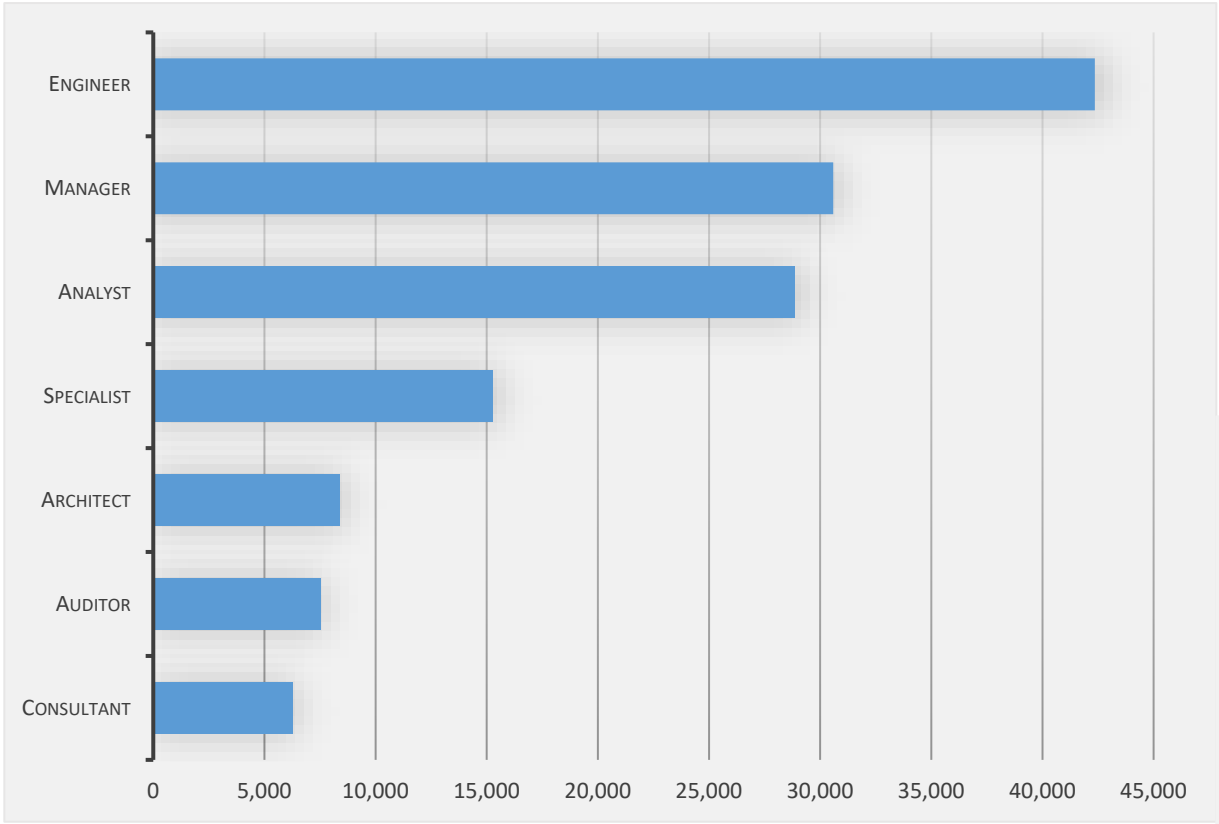
The greatest growth has been in the category Auditor. These individuals evaluate the preparedness of the information security systems. The growth rate (132% during the four year period 2010 to 2014) is a challenge for employers as they try to recruit from a constrained pool of talent. Job postings for this category remained open the longest of any CyberSecurity job category (43 days on average)

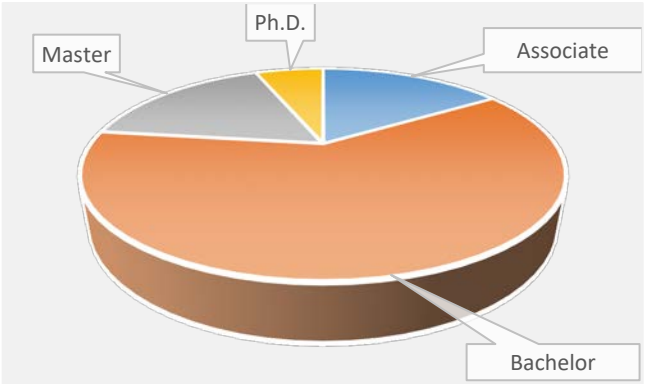
The most advanced roles are in the categories of Consultant, Engineer and Architect. The educational and certification requirements are significant for these roles, and they command the highest salaries of $95,311, $97,620, and $112,659, respectively.

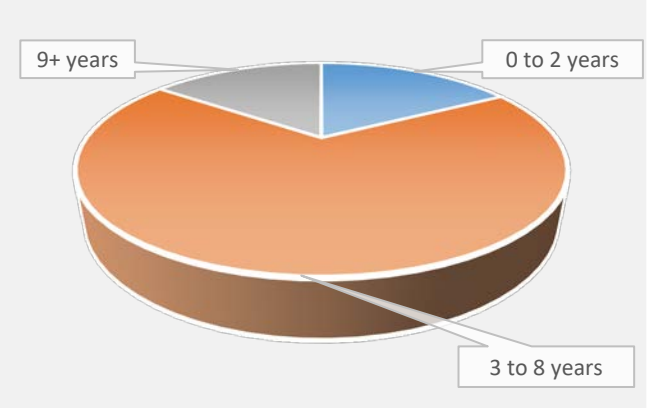
Occupational Categories and Representative Job Titles

Category & Description	Sample Job Titles
Engineer *Builds and maintains information security solutions for an organization's IT infrastructure.*	*Security Engineer* *Network Engineer* *Systems Engineer* *Software Development Engineer* *Network Security Engineer*
Manager *Develops and manages an organization's information security operations and infrastructure.*	*Systems Administrator* *Security Manager* *Network Administrator* *Security Administrator* *Information Security Manager*
Analyst *Detects and prevents cybersecurity threats by identifying weaknesses in an organization's information security.*	*Security Analyst* *Information Security Analyst* *Information Technology Security Analyst* *Compliance Analyst* *Operations Analyst*
Specialist *Implements, tests, and monitors an organization's information security systems.*	*Security Specialist* *Information Technology Specialist* *Information Security Specialist* *Network Specialist* *Cyber Security Specialist*
Architect *Oversees the design and implementation of an organization's information security systems.*	*Security Architect* *Solutions Architect* *Network Architect* *Enterprise Architect* *Information Security Architect*
Auditor *Conducts security audits to assess the effectiveness of an organization's information security protocols and infrastructure.*	*Information Technology Auditor* *Internal Auditor* *Staff Auditor* *Internal It Auditor* *It Auditor*
Consultant *Provides advice to inform the design and implementation of an organization's information security solutions.*	*Security Consultant* *Information Security Consultant* *Information Technology Consultant* *Technical Consultant* *Technology Consultant*

CyberSecurity Job Postings (238,158 Total)







Summary Statistics

	Total Postings	Growth (2010-2014)	Average Salary	Average Days Open
Overall	**238,158**	**91%**	**$83,934**	**40 Days**
Engineer	42,355	55%	$97,620	42 Days
Manager	30,586	80%	$90,262	41 Days
Analyst	28,853	100%	$78,898	38 Days
Specialist	15,289	97%	$80,847	35 Days
Architect	8,409	95%	$112,659	37 Days
Auditor	7,533	132%	$80,750	43 Days
Consultant	6,294	44%	$95,311	31 Days

Professionals can enter the CyberSecurity workforce most easily in the job category of Specialist where there is a minimal educational requirement (37% of the postings are eligible to professionals with only 2 years of college education) and a minimal experience requirement (44% of the postings are eligible to candidates with less than 2 years of work experience.

Educational Requirements

	A.S.	B.S.	M.S.	Ph.D.
Overall	**38,073 (16%)**	**145,243 (61%)**	**40,918 (17%)**	**13,938 (6%)**
Engineer	7,082 (17%)	27,879 (66%)	5,591 (13%)	1,803 (4%)
Manager	4,245 (14%)	19,913 (65%)	5,251 (17%)	1,177 (4%)
Analyst	3,316 (11%)	21,514 (75%)	3,223 (11%)	799 (3%)
Specialist	5,639 (37%)	6,717 (44%)	1,364 (9%)	1,569 (10%)
Architect	1,617 (19%)	4,422 (53%)	1,981 (24%)	389 (5%)
Auditor	74 (1%)	4,907 (65%)	2,055 (27%)	496 (7%)
Consultant	671 (11%)	4,388 (70%)	1,076 (17%)	158 (3%)

Beyond the role of Specialist, entry into, and advancement within, the CyberSecurity workforce requires a commitment to both education and experience. Overall, more than 80% of the job postings required a bachelor degree; more than 20% require with a more advanced degree. Just as challenging, more than 80% of the job postings require at least 3 years of prior experience; 15% require more than 8 years of prior experience.

Experience Requirements

	0 to 2 years	3 to 8 years	9+ years
Overall	**40,334 (17%)**	**161,556 (68%)**	**36,282 (15%)**
Engineer	3,476 (8%)	31,882 (75%)	6,997 (17%)
Manager	3,179 (10%)	22,891 (75%)	4,516 (15%)
Analyst	5,608 (19%)	20,861 (72%)	2,384 (8%)
Specialist	6,661 (44%)	7,246 (47%)	1,382 (9%)
Architect	302 (4%)	5,356 (64%)	2,751 (33%)
Auditor	2,361 (31%)	5,017 (67%)	155 (2%)
Consultant	1,222 (19%)	4,345 (69%)	728 (12%)

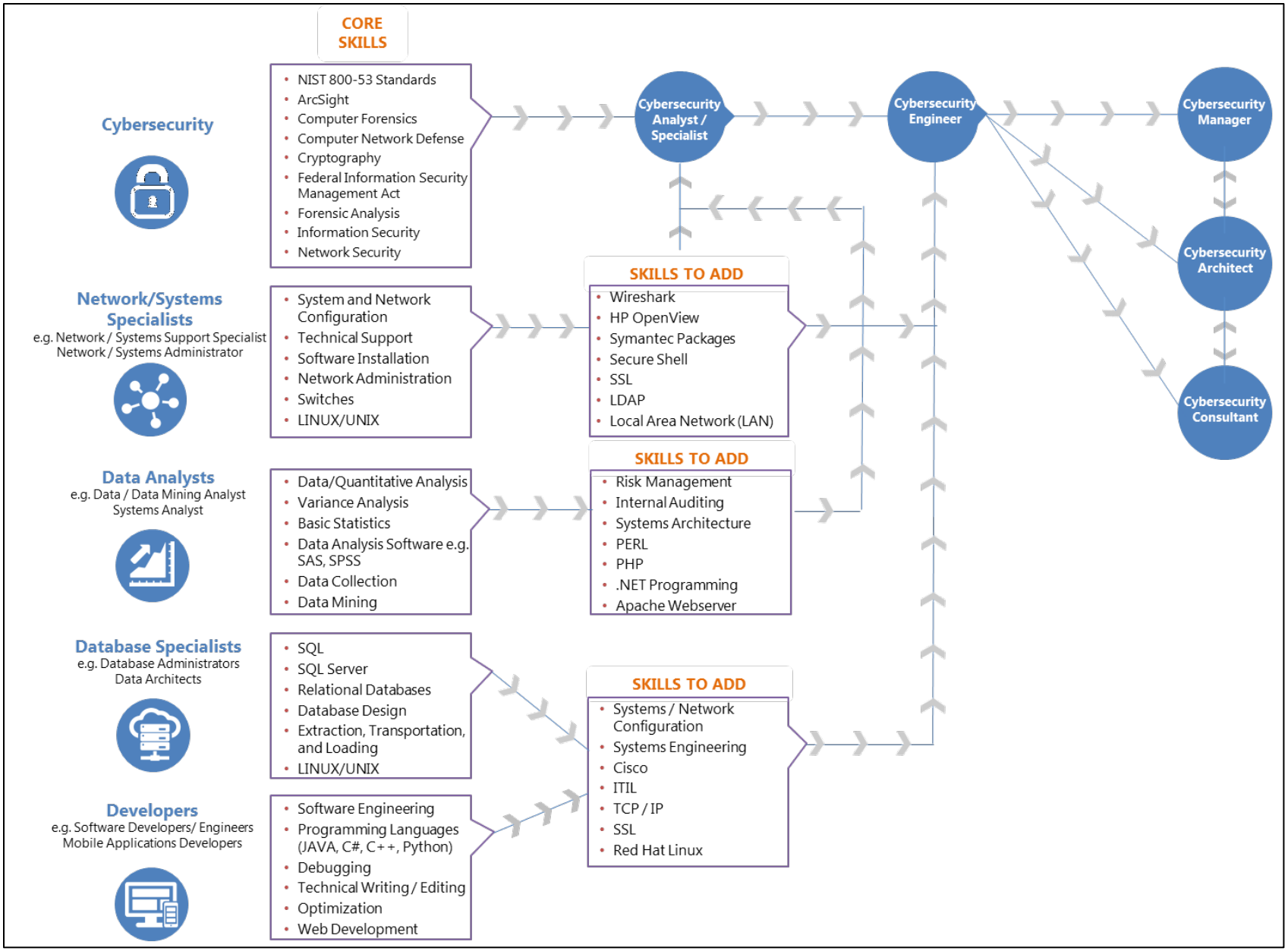
Career Pathways and Transitions

CyberSecurity is an emerging discipline that builds upon the skills of data analytics, data management, software development, digital networking and IT administration. Candidates, with these skills, have the opportunity to transition into the CyberSecurity workforce with additional training, education and certification.

The normative career pathway begins with the role of Specialist, as this role requires the least amount of education and experience. This role is a natural entry-point for workers with experience in digital networking, administration and/or technical support.

The role of Analyst can also be an entry point for workers with experience in data analytics.

For workers advancing in the career pathway, the role of Network Engineer is a frequent, and almost universal, stop along the way. Advancing in the career pathway, to a lesser IT administration. It can also be an entry-point for workers skilled and experienced in Database Management and/or Software Developmen


CORE SKILLS
Cybersecurity
NIST 800-53 Standards
ArcSight
Computer Forensics
Computer Network Defense
Cryptography
Federal Information Security Management Act
Forensic Analysis
Information Security
Network Security
Cybersecurity Analyst / Specialist
Cybersecurity Engineer
Cybersecurity Manager
Cybersecurity Architect
Cybersecurity Consultant
Network/Systems Specialists
e.g. Network / Systems Support Specialist
Network / Systems Administrator
System and Network Configuration
Technical Support
Software Installation
Network Administration
Switches
LINUX/UNIX
SKILLS TO ADD
Wireshark
HP OpenView
Symantec Packages
Secure Shell
SSL
LDAP
Local Area Network (LAN)
Data Analysts
e.g. Data / Data Mining Analyst
Systems Analyst
Data/Quantitative Analysis
Variance Analysis
Basic Statistics
Data Analysis Software e.g. SAS, SPSS
Data Collection
Data Mining
SKILLS TO ADD
Risk Management
Internal Auditing
Systems Architecture
PERL
PHP
.NET Programming
Apache Webserver
Database Specialists
e.g. Database Administrators
Data Architects
SQL
SQL Server
Relational Databases
Database Design
Extraction, Transportation, and Loading
LINUX/UNIX
SKILLS TO ADD
Systems / Network Configuration
Systems Engineering
Cisco
ITIL
TCP / IP
SSL
Red Hat Linux
Developers
e.g. Software Developers/ Engineers
Mobile Applications Developers
Software Engineering
Programming Languages (JAVA, C#, C++, Python)
Debugging
Technical Writing / Editing
Optimization
Web Development

Career transitions, in CyberSecurity, is not casual nor easy to make. Each advancement requires additional skills (often specific to CyberSecurity) and a rigorous set of industry certifications.

The most senior positions in the career pathway are the roles of Manager, Architect, Consultant, or Chief Security Officer. Many of these positions report to the organization's most senior management and are responsible for either operations or strategy as it applies to a large department or the entire organization.

Opportunities for Veterans

The field of CyberSecurity can be a logical career pathway for returning veterans. The security clearance credentials, possessed by many veterans, imply a clearance eligibility that many civilian workers may, or may not, possess.

Approximately 11% of CyberSecurity job posting require some kind of security clearance, and these jobs take employers longer to fill (10% longer than CyberSecurity jobs that do not have a security clearance requirement).

The following table lists the job titles of military occupations which require skills found in a high percentage of civilian CyberSecurity job postings. This information can be used to identify military personnel most likely make successful transitions into civilian cybersecurity roles.

MOC	MOC Title	Service	Career
275	Information Systems Technician	Coast Guard	Enlisted
6049	NALCOMIS Application Administrator/Analyst	Marine Corps	Enlisted
9556	Security Specialist	Navy	Enlisted
17C0	Cyberspace Operations Commander	Air Force	Officer
17D1x, 17D3x, 17D4x	Cyberspace Operations	Air Force	Officer
140A	Command and Control Systems Integrator	Army	Officer
24A	Telecommunications Systems Engineer	Army	Officer
24X	Designated Telecommunications Systems Engineer	Army	Officer
250A	Telecommunications Technician	Army	Officer
254A	Signal Systems Support Technician	Army	Officer
255S	Information Protection Technician	Army	Officer
25A	Signal, General	Army	Officer
290A	Electronic Warfare Technician	Army	Officer
29A	Electronic Warfare Officer	Army	Officer
352N	Signals Intelligence Analysis Technician	Army	Officer
352S	Signals Collection Technician	Army	Officer
35G	Signal Intelligence/Electronic Warfare	Army	Officer
0206	Signal Intelligence/Ground Electronic Warfare Officer	Marine Corps	Officer
0602	Communications Officer	Marine Corps	Officer
0603	Command, Control, Communications, Computers and Intelligence (C4I) Planner Officer	Marine Corps	Officer
0610	Telecommunication Systems Engineering Officer	Marine Corps	Officer
0620	Tactical Communications Planning and Engineer Officer	Marine Corps	Officer
0640	Spectrum Management Officer	Marine Corps	Officer
2602	Signals Intelligence/Electronics Warfare Officer	Marine Corps	Officer
2802	Electronics Maintenance Officer (Ground)	Marine Corps	Officer
8858	Command, Control, Communications, Computers and Intelligence (C4I) Officer	Marine Corps	Officer
9650	Electronic Intelligence Officer	Marine Corps	Officer
9658	Command, Control, Communications, Computers and Intelligence (C4I) Officer	Marine Corps	Officer
2748	Security Manager, Information Security Program	Navy	Officer
9046	Staff Electronic Warfare Officer	Navy	Officer
9282	Ship's Electronic Warfare Officer	Navy	Officer
9404	Tactical Deception Plans Officer	Navy	Officer
9510	Communications System Center Director	Navy	Officer
9512	Communications System Current Ops Manager	Navy	Officer
9515	Communications Plans & Operations Officer	Navy	Officer
9517	Communication Security Officer	Navy	Officer
9523	Joint Interface Control Officer	Navy	Officer
9525	Communication Watch Officer	Navy	Officer
9530	Cryptoboard Officer	Navy	Officer
9543	Director of Communications	Navy	Officer
9560	Satellite Communications Officer	Navy	Officer
9575	Circuit Control Officer	Navy	Officer
9582	Information Systems Officer	Navy	Officer
9590	Staff Communications Officer	Navy	Officer
9595	Communications Traffic Officer	Navy	Officer
9690	Intelligence Support to CNO/CYBER	Navy	Officer
9781	ADP Systems Security Officer	Navy	Officer
2748	Security Manager, Information Security Program	Navy	Officer

IMPLICATIONS AND RECOMMENDATIONS

The CyberSecurity career pathway offers strong opportunity for both first time and recurring job seekers. It features high demand, significant growth and high levels of compensation.

The workforce issues in CyberSecurity are significant for most companies and organizations. Several factors, including higher than normal growth rates, limited CyberSecurity talent, and a lengthy process of education and certification, combine to make it difficult to find qualified talent and extend the time required to fill open positions.

The workforce issues are best addressed by coordinated effort of educators, employers, and policymakers. To that end, this analysis suggests that the following concrete steps are all steps in "the right direction":

- **Transition existing workers into a CyberSecurity pathway:** Many of the roles in CyberSecurity require skills and competencies which have traditionally been required of network administrators, data management specialists and system engineers. The employees in these positions can, with additional training, skill development and certification, be transitioned into a career pathway in CyberSecurity.
- **Resist the temptation to "OverSpec" the job description:** Employers pride themselves on their ability to find and recruit the best talent. And while specifying more than "what is needed" may appear to be one way to do this, it has proven to backfire in this field where talent is in short supply. The CISSP certification, by example, is difficult to obtain and individuals who possess it are in high demand. Employers who include this as either a required or desired credential must be prepared to offer elevated strategies and senior level job titles or else risk finding that their recruitment efforts are both prolonged and unsatisfied.
- **Upgrade educational programs improving their relevancy and authenticity:** Employers prefer to hire candidates who possess critical thinking skills, are able to work on team projects and have some level of work experience. Quality educational programs address all of these attributes challenging and exposing their students to each of these areas aided by industry advisors and their companies. The very best educational programs require and facilitate placement in Cyber-related internship as part of the program and degree requirement.
- **Promote the value of a career in CyberSecurity:** Students and job seekers need to better understand the magnitude and value of the opportunity in cybersecurity. Employers and educators are competing with rival fields for students and employees, and students would benefit from more information about the rewards and responsibilities of a career protecting the nation's digital information.

SPECIFIC PROFILES

Engineer

Engineers build and maintain the security architecture for the IT infrastructure. This is the largest job category in CyberSecurity (42,355 job postings). It grew 55% in the four year period 2010 to 2014, and while robust, this growth rate was significantly lower than almost any other category. Job postings, in this category, remained open an average of 42 days, and the average salary was nearly $14,000 higher than the average salaries across the CyberSecurity spectrum.

Summary Statistics

	Total Postings	Growth (2010-2014)	Average Salary	Average Days Open
Engineer	42,355	55%	$97,620	42 Days

Most job postings (more than 80%) for CyberSecurity Engineers require a four year degree; 17% require a graduate level degree. A modest opportunity (less than 20% of the job postings) exists for candidates with an associate degree.

Educational Requirements

	A.S.	B.S.	M.S.	Ph.D.
Engineer	7,082 (17%)	27,879 (66%)	5,591 (13%)	1,803 (4%)

The vast majority of job postings (more than 90%) for CyberSecurity Engineers require at least 3 years of prior experience; 17% require at least 8 years of prior experience. There is a modest opportunity (3,476 job postings) for few entry-level positions in this category, but these positions can be difficult to find (as they are less than 10% of the total).

Experience Requirements

	0 to 2 years	3 to 8 years	9+ years
Engineer	3,476 (8%)	31,882 (75%)	6,997 (17%)

Industry certifications are a valued credential and can significantly affect an employer's level of interest in a specific candidate. It can be a competitive advantage differentiating two candidates who are comparable in experience and education; or it can disqualify a candidate for certain positions that require it. Job Postings are increasingly explicit about the need for specific certifications, and in the case of the one certification, the vendor neutral Certified Information Systems Security Professional (CISSP) certification, more than 20% of the job postings for the role of Engineer, specified this certification as a requirement.

Top Certifications

Certification	Postings	Percent of Title Area
Certified Information Systems Security Professional (CISSP)	9,524	22%
Cisco Certified Network Associate	5,320	13%
Cisco Certified Network Professional (CCNP)	5,080	12%
Security+	2,849	7%
Cisco Certified Internetwork Expert (CCIE)	2,548	6%
Microsoft Certified Systems Engineer (MCSE)	2,011	5%
Certified Information Security Manager (CISM)	1,893	4%
Certified Information Systems Auditor (CISA)	1,761	4%
Cisco Certified Security Professional	1,030	2%
GIAC Security Essentials	996	2%

The role of Engineer requires a set of skills unique to CyberSecurity, including an in-depth understanding of firewalls, network and information security, and cryptography. It also relies on more generic software and programming skills and a familiarity with device and software configuration, systems engineering, and network administration. The Cisco Networking Academy is a popular curriculum, adopted by many schools and universities, as a platform of learning modules in this area.

Top Skills

Baseline Skills	Specialized Skills	Software and Programming Skills
Communication Skills	Firewalls	Cisco
Troubleshooting	Network Security	LINUX
Writing	Network Engineering	TCP-IP Protocol
Planning	Information Security	UNIX
Organizational Skills	Cryptography	Virtual Private Networking (VPN)
Problem Solving	System and Network Configuration	Domain Name System (DNS)
Research	Systems Engineering	JAVA
Project Management	Wide Area Network (WAN)	PERL
Customer Service	Software Engineering	Python
Detail-Oriented	Technical Support	SQL
Quality Assurance and Control	Network Administration	OSPF
Microsoft Office	Information Assurance	SSL
Presentation Skills	System Administration	C++
Multi-Tasking	VoIP	Oracle
Microsoft Visio	Telecommunications	Dynamic Host Configuration Protocol (DHCP)
Change Management	Technical Writing - Editing	ITIL
Leadership	Software Installation	CISA
Microsoft Excel	Disaster Recovery Planning	Cisco Routers
Time Management	EIGRP	JavaScript
Analytical Skills	Configuration Management	Extensible Markup Language (XML)

There is a large demand for Engineers in all of the major cities (the nation's capital more than any other) however the hubs of Colorado Springs, and San Jose have a particularly high concentration of jobs (more than 6 times the national average).

Top Metropolitan Areas

Location Analysis

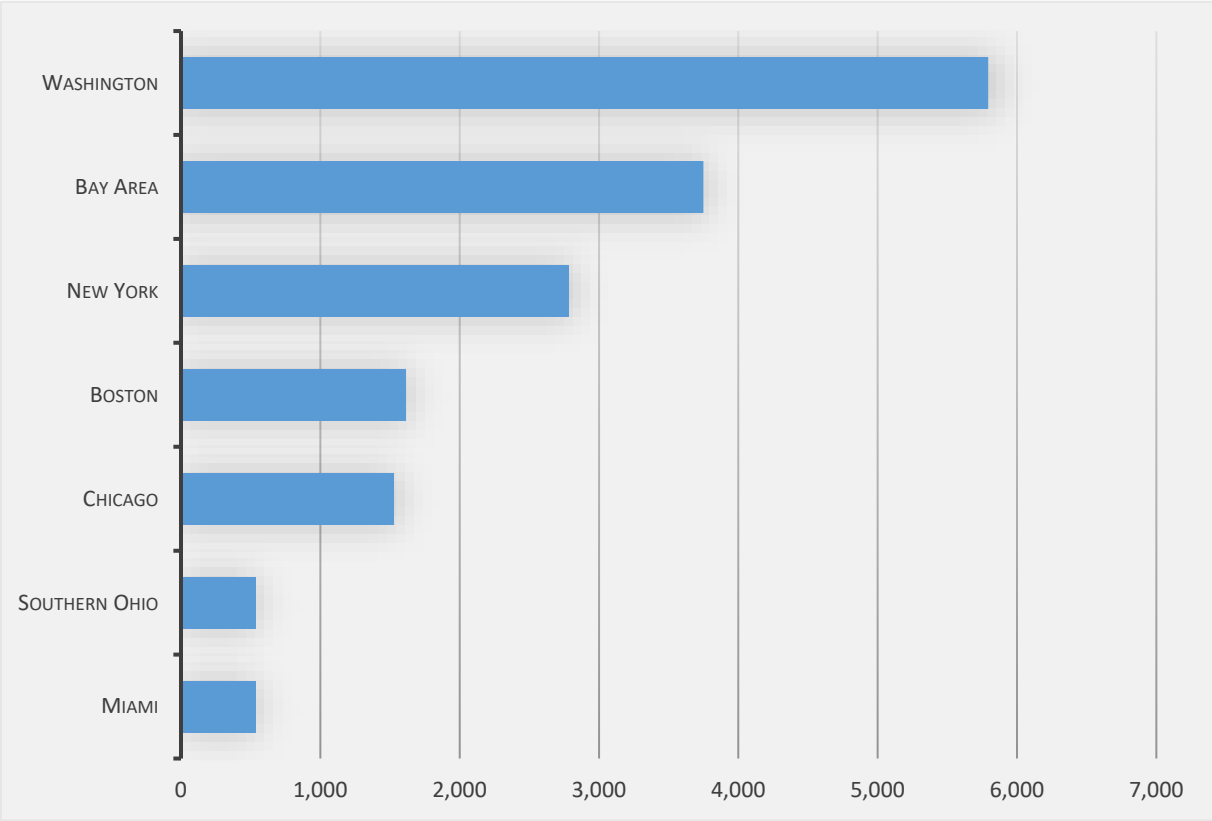
Metro Area	Postings
Washington, D.C	5,793
New York	2,778
San Jose	1,900
San Francisco	1,849
Dallas	1,686
Boston	1,608
Chicago	1,527
Los Angeles	1,373
Atlanta	1,310
Baltimore	1,135

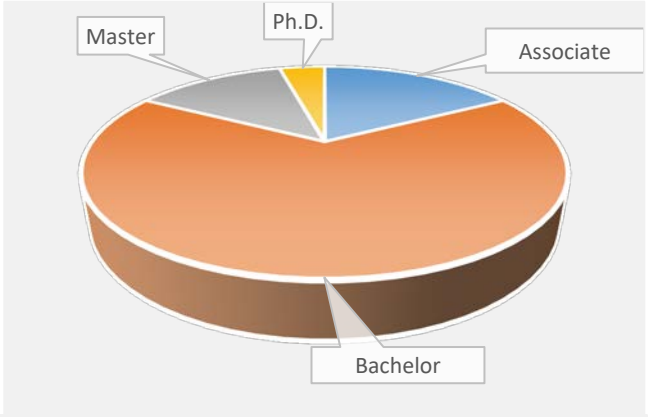
Metro Area	Location Quotient
Colorado Springs	6.7
Washington, D.C.	6.3
San Jose	6.2
Huntsville, AL	3.4
Baltimore	2.8
San Francisco	2.8
Boulder	2.7
Durham	2.7
Denver	2.3
Raleigh	2.1

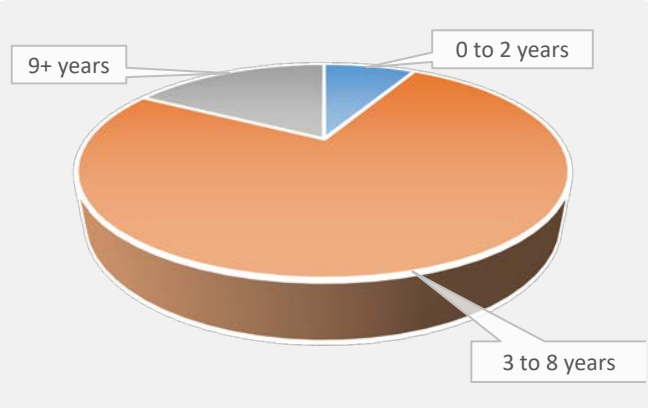
The employment market is maturing at different rates in different regions. Two regions (Washington D.C. and the Bay Area of San Jose) have large numbers of job postings and significant concentration density. Other regions (Miami and Chicago) have smaller numbers but higher growth rates.

It is worth noting that the concentration of job postings is higher than the national average in all of the markets analyzed for this study. It is also worth noting that the posting duration, in these same urban areas is lower than the national average, and only slightly higher than the posting duration for IT jobs overall. The only exception to this trend is Boston, which has a higher than average (45 days) posting duration for Engineers.

Job Postings for Engineers (42,355 Nationally)







	Total Postings	Growth (2010 to 2014)	Average Salary	Average Days Open	Location Quotient
Nationally	**42,355**	**55%**	**$97,620**	**42 Days**	**1.0**
Bay Area	3,749	61%	$115,418	39 Days	3.9
Boston	1,608	97%	$102,920	45 Days	2.0
Chicago	1,527	143%	$103,993	39 Days	1.1
Miami	532	173%	$87,975	34 Days	0.7
New York	2,778	89%	$107,440	34 Days	1.0
Southern Ohio	533	118%	$91,393	29 Days	0.7
Washington, D.C.	5,793	13%	$101,233	37 Days	6.3

The majority of job postings (75%) for Engineers require a Bachelor's Degree, but opportunities do exist for candidates with an Associate's Degree. Opportunities exist for candidates with Associate Degrees in modest number (Washington, New York and the Bay Area having the largest number of postings). The Bay Area has the notable distinction of requiring Graduate Degrees for more job postings (36% of all postings, more than twice the national average) than any other region.

	A.S.	B.S.	M.S.	Ph.D.
Nationally	**7,082 (17%)**	**27,879 (66%)**	**5,591 (13%)**	**1,803 (4%)**
Bay Area	466 (12%)	1,906 (51%)	1,060 (28%)	316 (8%)
Boston	207 (13%)	993 (62%)	283 (18%)	125 (8%)
Chicago	339 (22%)	1,013 (66%)	145 (9%)	31 (2%)
Miami	84 (16%)	310 (58%)	130 (24%)	9 (2%)
New York	500 (18%)	1,878 (68%)	312 (11%)	87 (3%)
Southern Ohio	103 (19%)	364 (68%)	51 (10%)	14 (3%)
Washington, D.C.	736 (13%)	4,013 (69%)	750 (13%)	295 (5%)

This category has limited opportunity for entry-level professionals as postings consistently require a modest work experience (75% to 80% calling for more than 3 years of experience). Washington D.C. is no exception (72% of postings require more than 3 years of experience), however a high number (25% of postings) require more than 9 years of work experience. This statistic is 50% higher than the national norm and may be a consequence of the region's high concentration of defense contractors and federal government workers.

	0 to 2 years	3 to 8 years	9+ years
Nationally	**3,476 (8%)**	**31,882 (75%)**	**6,997 (17%)**
Bay Area	309 (8%)	3,000 (80%)	441 (12%)
Boston	124 (8%)	1,255 (78%)	229 (14%)
Chicago	111 (7%)	1,212 (79%)	204 (13%)
Miami	44 (8%)	423 (80%)	65 (12%)
New York	223 (8%)	2,256 (81%)	299 (11%)
Southern Ohio	41 (8%)	406 (76%)	86 (16%)
Washington, D.C.	462 (8%)	3,833 (66%)	1,498 (26%)

Manager

Managers are responsible for both the information security infrastructure and the personnel who design and administer the operation of it. This is the second largest cybersecurity category (more than 30,000 postings). The opportunity for Managers grew significantly (80% growth) in the four year period 2010 to 2014. This job category pays well (average salary is $90,262), and new positions can be challenging to fill (41 days average duration for job postings).

Summary Statistics

	Total Postings	Growth (2010-2014)	Average Salary	Average Days Open
Manager	30,586	80%	$90,262	41 Days

The educational requirements for this category do not differ from those of the other categories (86% require a bachelor degree, 25% a more advanced degree).

Educational Requirements

	A.S.	B.S.	M.S.	Ph.D.
Manager	4,245 (14%)	19,913 (65%)	5,251 (17%)	1,177 (4%)

However the experience requirement is much more rigorous (90% of job openings require at least 3 years of experience, 15% require at least 9 years of experience).

Experience Requirements

	0 to 2 years	3 to 8 years	9+ years
Manager	3,179 (10%)	22,891 (75%)	4,516 (15%)

Managers are required to have a strong mix of systems and networking skills (e.g. systems administration and network security) and a demonstrated proficiency in both organizational and interpersonal skills (project management, planning, and communications).

Top Skills

Baseline Skills	Specialized Skills	Software and Programming Skills
Communication Skills	Information Security	LINUX
Organizational Skills	Network Security	UNIX
Planning	Systems Administration	Oracle
Troubleshooting	Firewalls	Cisco
Writing	System and Network Configuration	SQL
Project Management	Technical Support	Domain Name System (DNS)
Problem Solving	Software Installation	Transmission Control Protocol - Internet Protocol (TCP - IP)
Research	Cryptography	ITIL
Customer Service	Network Administration	Virtual Private Networking (VPN)
Microsoft Office	Disaster Recovery Planning	Dynamic Host Configuration Protocol (DHCP)
Building Effective Relationships	Risk Management	Microsoft SharePoint
Microsoft Excel	Internal Auditing	SAP
Detail-Oriented	Wide Area Network (WAN)	Microsoft Exchange
Presentation Skills	Windows Server	Red Hat Linux
Change Management	Database Administration	SQL Server
Budgeting	Business Process	PERL
Supervisory Skills	Risk Assessment	JAVA
Project Planning and Development Skills	Telecommunications	Microsoft SQL
Leadership	Optimization	Solaris
Quality Assurance and Control	Hardware and Software Configuration	Symantec Packages

The certification requirements for this category are not unique when compared to other jobs categories, however certain job postings (15 to 20%) will require either a CISSP or CISA.

These certifications are noteworthy because they require documentation demonstrating at least five years of work experience.

Top Certifications

Certification	Postings	Percent of Title Area
Certified Information Systems Security Professional (CISSP)	5,690	19%
Certified Information Systems Auditor (CISA)	5,224	17%
Security+	3,204	10%
Certified Information Security Manager (CISM)	2,411	8%
Microsoft Certified Systems Engineer (MCSE)	2,122	7%
Project Management Certification (E.G. PMP)	1,620	5%
Cisco Certified Network Associate	1,511	5%
Cisco Certified Network Professional (CCNP)	1,468	5%
GIAC Security Essentials	1,180	4%

Top Metropolitan Areas

Metro Area	Postings
Washington, D.C.	3,094
New York	2,468
Chicago	1,210
Dallas	1,173
Los Angeles	1,159
San Francisco	922
Boston	872
Atlanta	837
San Jose	744

Metro Area	Location Quotient
Washington, D.C.	4.6
San Jose	3.4
Denver	2.1
San Francisco	1.9
Charlotte	1.9
Baltimore	1.7
Portland	1.7
Dallas	1.6
Virginia Beach	1.6

The strongest demand for Managers is in the defense and technology hubs of Washington, D.C. and San Francisco. There is also a strong concentration of job openings in the metro areas of Denver, Charlotte, and Portland.

Location Analysis

The areas of Miami and Chicago have experienced the highest level of job growth in this category (145% and 152%, respectively since 2010). They also have high average posting durations (41 and 43 days, respectively). This suggests that the supply of qualified workers is struggling to keep up with demand in these locations.

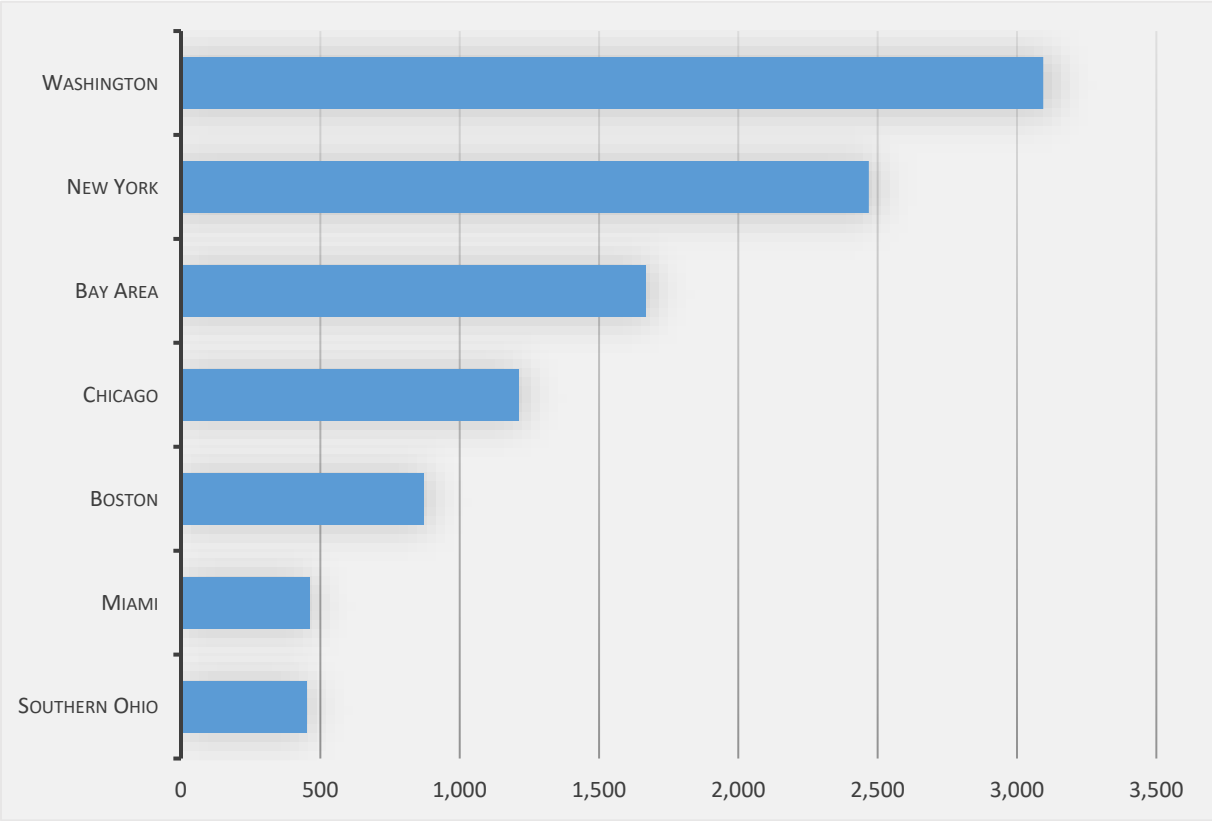
The metro areas of Washington and New York have the largest number of postings, and Washington has an extremely high location quotient (over 4 times the national average).

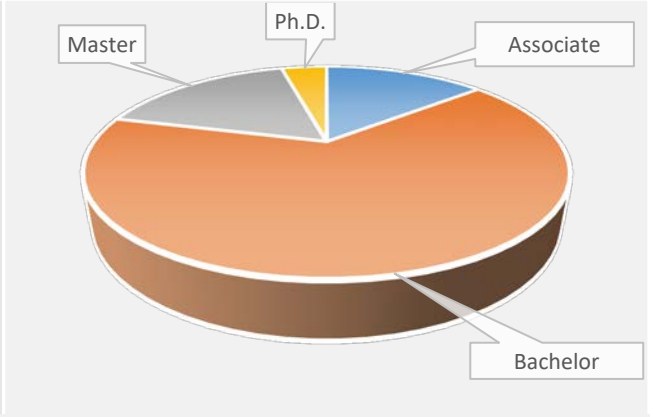
Managers, in CyberSecurity are well paid, and the managers in the selected metro areas are, with the exception of Southern Ohio, paid 10% to 15% more than the national average of $90,262.

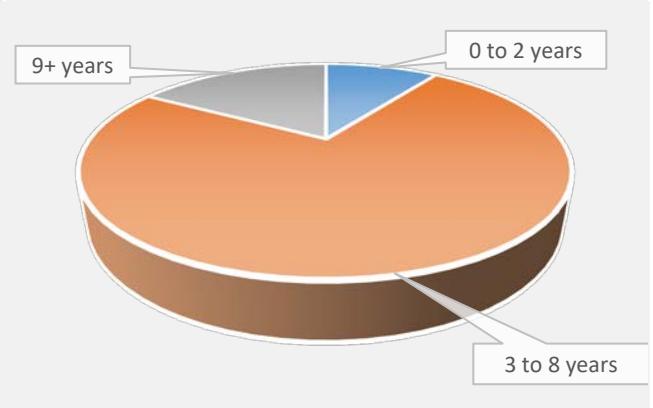
	Total Postings	Growth (2010 to 2014)	Average Salary	Average of Days Open	Location Quotient
Nationally	**30,586**	**80%**	**$90,262**	**41 Days**	**1.0**
Bay Area	1,666	65%	$100,304	40 Days	2.4
Boston	872	67%	$103,302	37 Days	1.5
Chicago	1,210	145%	$106,640	41 Days	1.2
Miami	461	152%	$96,239	43 Days	0.9
New York	2,468	81%	$108,481	37 Days	1.3
Southern Ohio	449	94%	$79,183	27 Days	0.8
Washington, D.C.	3,094	47%	$98,282	37 Days	4.6

A bachelor's degree is, generally, an important credential (both in CyberSecurity and in the Manager category) but in Boston, Miami, New York, and the Bay Area employers place even greater emphasis (more than 90% of all openings) on a four-year degree for Manager candidates.

Job Postings for Managers (30,586 Nationally)







	A.S.	B.S.	M.S.	Ph.D.
Nationally	**4,245 (14%)**	**19,913 (65%)**	**5,251 (17%)**	**1,177 (4%)**
Bay Area	133 (8%)	1,026 (62%)	409 (25%)	98 (6%)
Boston	60 (7%)	574 (66%)	187 (21%)	51 (6%)
Chicago	145 (12%)	755 (62%)	256 (21%)	54 (4%)
Miami	35 (8%)	337 (73%)	89 (19%)	0 (0%)
New York	147 (6%)	1,647 (67%)	537 (22%)	137 (6%)
Southern Ohio	69 (15%)	283 (63%)	86 (19%)	11 (3%)
Washington, D.C.	388 (13%)	2,224 (72%)	393 (13%)	89 (3%)

Job openings, nationally, specify a minimum of 3 years of experience for most (90%) manager positions. The metro areas, analyzed for this report, were, as a general rule, slightly more rigorous (with more than 90% specify a minimum of 3 years of experience).

	0 to 2 years	3 to 8 years	9+ years
Nationally	**3,179 (10%)**	**22,891 (75%)**	**4,516 (15%)**
Bay Area	106 (6%)	1,293 (78%)	266 (16%)
Boston	66 (8%)	718 (82%)	88 (10%)
Chicago	76 (6%)	942 (78%)	192 (16%)
Miami	30 (7%)	374 (81%)	57 (12%)
New York	184 (7%)	1,947 (79%)	336 (14%)
Southern Ohio	34 (8%)	364 (81%)	50 (11%)
Washington, D.C.	310 (10%)	2,177 (70%)	607 (20%)

Washington D.C., although consistent with the national trend for job postings requiring more than three years of experience, led both the nation and the other metro areas requiring more than 9 years of experience for 20% of the open Manager positions.

Analyst

Analysts detect and prevent cybersecurity threats by identifying vulnerabilities in the infrastructure. This is the third largest cybersecurity category (almost 29,000 postings) The opportunity for Analysts grew significantly (100% growth) in the four year period 2010 to 2014. This job category has an average salary of $78,898 and job postings remain open for 38 days on average.

Summary Statistics

	Total Postings	Growth (2010-2014)	Average Salary	Average Days Open
Analyst	28,853	100%	$78,898	38 Days

Most job postings, in this category, specify the the requirement for a bachelor's degree (75% of all job postings), while only a modest number (14% require a more advanced degree).

Educational Requirements

	A.S.	B.S.	M.S.	Ph.D.
Analyst	3,316 (11%)	21,514 (75%)	3,223 (11%)	799 (3%)

However, the experience requirement is much more rigorous (90% of job openings require at least 3 years of experience, 15% require at least 9 years of experience).

The Analyst position is a strong candidate for entry level professionals (almost 20% of the Analyst postings specify 0 to 3 years of prior experience).

Experience Requirements

	0 to 2 years	3 to 8 years	9+ years
Analyst	5,608 (19%)	20,861 (72%)	2,384 (8%)

Analysts are required to have specialized skills in information security, firewalls, network security, and cryptography and a demonstrated proficiency in the baseline skills of communication, writing, organization and problem solving. They are expected to have programming experience in SQL and Python, and a background in data mining and manipulation.

Top Skills

Baseline Skills	Specialized Skills	Software and Programming Skills
Communication Skills	Information Security	LINUX
Writing	Firewalls	UNIX
Organizational Skills	Network Security	SQL
Problem Solving	Cryptography	Transmission Control Protocol - Internet Protocol (TCP - IP)
Research	Technical Support	Cisco
Project Management	System and Network Configuration	Oracle
Troubleshooting	Information Assurance	ITIL
Planning	Systems Analysis	Virtual Private Networking (VPN)
Microsoft Excel	Business Process	JAVA
Microsoft Office	HIPAA	PERL
Customer Service	Risk Management	Microsoft SharePoint
Detail-Oriented	Business Analysis	Domain Name System (DNS)
Microsoft PowerPoint	System Administration	Python
Multi-Tasking	Risk Assessment	SAP
Analytical Skills	Network Engineering	Symantec Packages
Building Effective Relationships	Technical Writing - Editing	ArcSight
Quality Assurance and Control	Disaster Recovery Planning	McAfee
Time Management	Wide Area Network (WAN)	Microsoft Operating Systems
Presentation Skills	Telecommunications	SSL
Change Management	Data Analysis	C++

Candidates, who are certified as CISSPs, will have an advantage when applying for positions in this category.

Top Certifications

Certification	Postings	Percent of Title Area
Certified Information Systems Security Professional (CISSP)	7,050	24%
Certified Information Systems Auditor (CISA)	3,491	12%
Certified Information Security Manager (CISM)	2,289	8%
Security+	1,513	5%
Cisco Certified Network Associate	1,068	4%
GIAC Certified Incident Handler	882	3%
GIAC Security Essentials	747	3%
Certified In Risk And Information Systems Control	723	3%
GIAC Certified Intrusion Analyst	667	2%
Microsoft Certified Systems Engineer (MCSE)	577	2%

The greatest demand, for this job category, in in the metro areas of Washington D.C. and New York. There is a high concentration of postings in the metro areas Charlotte, Denver, Baltimore, Austin, and San Jose (almost twice the national average).

Top Metropolitan Areas

Metro Area	Postings
Washington, D.C.	2,817
New York	1,853
Chicago	1,068
Dallas	1,040
Atlanta	794
San Francisco	686
Philadelphia	664
Los Angeles	662
Boston	658
Denver	642

Metro Area	Location Quotient
Washington, D.C.	4.5
Charlotte	2.6
Denver	2.3
Baltimore	2.2
Austin	1.9
San Jose	1.9
St. Louis	1.8
Portland, OR	1.8
Atlanta	1.6
Dallas	1.5

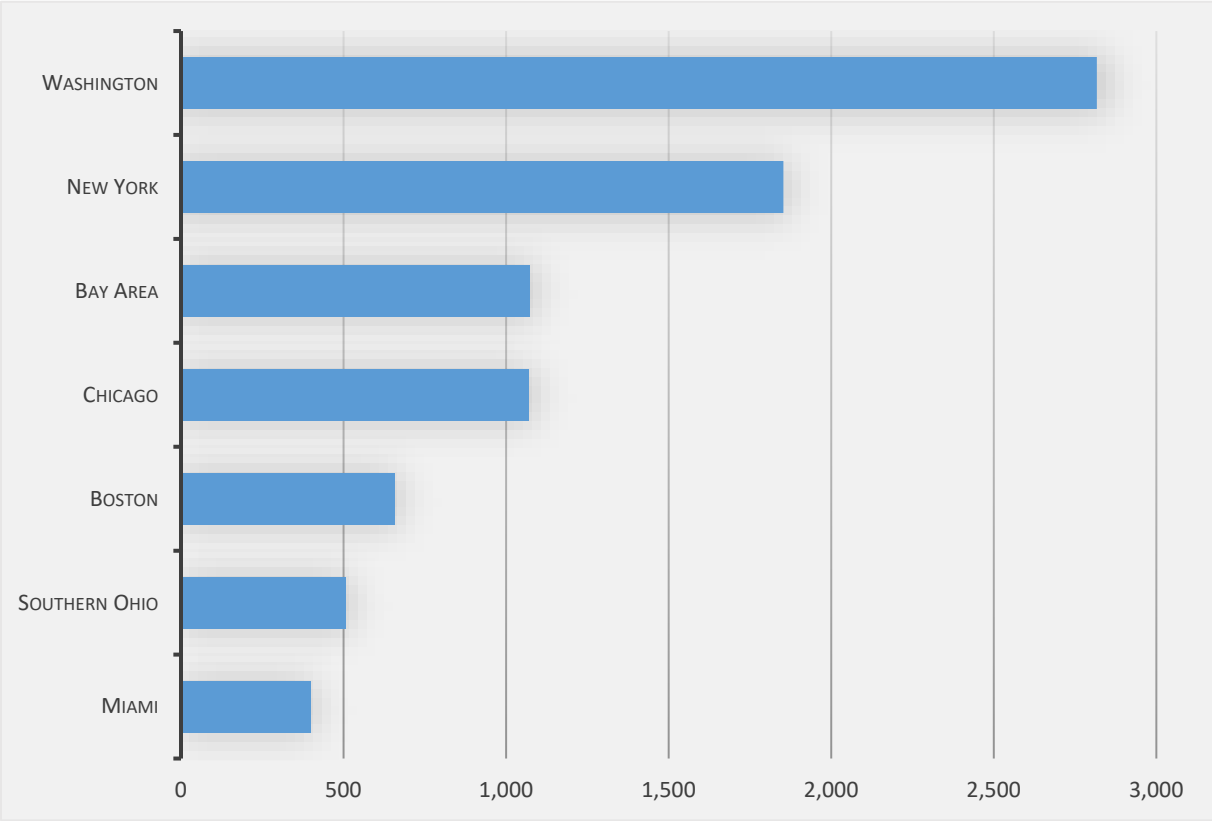
Location Analysis

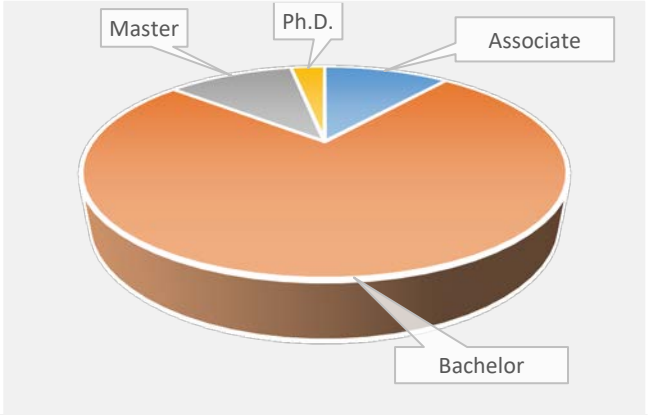
The areas of Chicago, Boston and Miami have experienced the highest level of job growth in this category (286%, 147% and 146%, respectively since 2010).

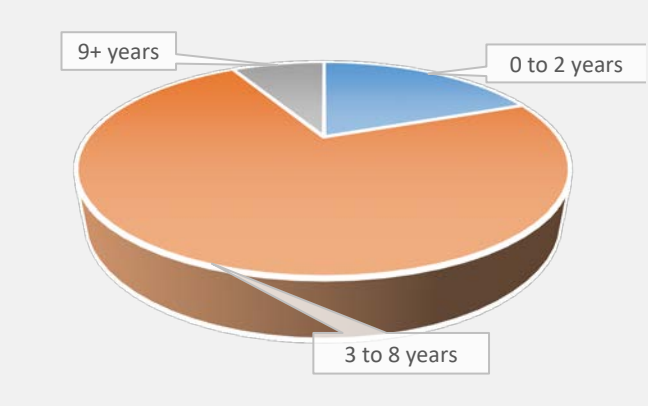
The metro areas of Washington and New York have the largest number of postings, and Washington has an extremely high location quotient (over 4 times the national average).

Analysts in the selected metro areas are, with the exception of Southern Ohio, paid 15% to 25% higher than the national average of $78,.898.

Job Postings for Analysts (28,853 Nationally)







	Total Postings	Growth (2010 to 2014)	Average Salary	Average Days Open	Location Quotient
Nationally	**28,853**	**100%**	**$78,898**	**38 Days**	**1.0**
Bay Area	1,073	126%	$94,886	42 Days	1.6
Boston	658	147%	$89,381	35 Days	1.2
Chicago	1,068	286%	$86,885	39 Days	1.1
Miami	399	146%	$67,732	37 Days	0.8
New York	1,853	72%	$101,241	36 Days	1.0
Southern Ohio	507	137%	$67,900	33 Days	1.0
Washington, D.C.	2,817	7%	$94,387	37 Days	4.5

The metro areas of Employers are predominantly looking to fill analyst openings with bachelor's-level candidates across geographies. In all locations, over 85% of openings request at least four-year degree, and in the Bay Area, Boston, New York, and Washington, D.C. this requirement is demanded in over 90% of openings. Only Miami and Southern Ohio show slightly greater opportunities for sub-baccalaureate workers, but the opportunities are still scarce compared to many other cybersecurity roles. In the Bay Area and New York, over 20% of postings request candidates with at least a master's degree

	A.S.	B.S.	M.S.	Ph.D.
Nationally	**3,316 (11%)**	**21,514 (75%)**	**3,223 (11%)**	**799 (3%)**
Bay Area	70 (7%)	753 (70%)	182 (17%)	67 (6%)
Boston	46 (7%)	503 (76%)	86 (13%)	23 (4%)
Chicago	117 (11%)	807 (76%)	115 (11%)	30 (3%)
Miami	48 (12%)	315 (79%)	32 (8%)	3 (1%)
New York	93 (5%)	1,323 (71%)	372 (20%)	65 (4%)
Southern Ohio	65 (13%)	384 (76%)	50 (10%)	8 (2%)
Washington, D.C.	137 (5%)	2,238 (79%)	355 (13%)	87 (3%)

Despite the lack of opportunities for workers without a bachelor's degree, entry-level opportunities are consistently more plentiful for Analysts. In Chicago and Southern Ohio the entry-level opportunities for Analysts are especially strong, with over 25% of openings requesting two or fewer years of experience in each location. In contrast, Washington, D.C. employers is the only geography where over 10% of Analyst openings request more than eight years of experience – in fact, Analyst openings in D.C. are over twice as likely to request workers with such heightened levels of experience than they are nationally.

	0 to 2 years	3 to 8 years	9+ years
Nationally	**5,608 (19%)**	**20,861 (72%)**	**2,384 (8%)**
Bay Area	195 (18%)	850 (79%)	28 (3%)
Boston	113 (17%)	509 (77%)	36 (5%)
Chicago	274 (26%)	742 (69%)	52 (5%)
Miami	46 (12%)	320 (80%)	33 (8%)
New York	280 (15%)	1,432 (77%)	140 (8%)
Southern Ohio	136 (27%)	351 (69%)	20 (4%)
Washington, D.C.	504 (18%)	1,837 (65%)	476 (17%)

Specialist

Specialists implement, test, and monitor an organization's information security systems. Specialist openings generally represent the strongest opportunities for workers to begin a career in cybersecurity due to strong opportunities for sub-baccalaureate and entry-level workers. In 2014 there were 15,289 openings for Specialists, representing 97% growth in demand since 2010. Because many Specialist openings represent entry-level opportunities, the average salary for Specialists is slightly below the average for all cybersecurity jobs. Nonetheless, it is still robust at just over $80,000. Specialists are also remaining open for 35 days – 13% shorter than the average for all cybersecurity roles. This suggests that the reduced education and experience requirements for these roles make them easier to fill than many of their counterparts in cybersecurity.

Summary Statistics

	Total Postings	Growth (2010-2014)	Average Salary	Average Days Open
Specialist	15,289	97%	$80,847	35 Days

Although a majority of postings for cybersecurity Specialists request at least a bachelor's, cybersecurity Specialists offer robust opportunities for workers without a four-year degree. In total, 37% of Specialist job postings were open to workers without a bachelor's degree – the highest among all cybersecurity job categories.

Educational Requirements

	A.S.	B.S.	M.S.	Ph.D.
Specialist	5,639 (37%)	6,717 (44%)	1,364 (9%)	1,569 (10%)

Just as Specialists offer strong opportunities for sub-baccalaureate workers, they also offer excellent opportunities for entry-level candidates. Almost half of all Specialist openings – 44%, specifically – were open to workers with two years or less experience. This establishes Specialists as the strongest option for inexperienced workers aiming to begin a career in cybersecurity.

Experience Requirements

	0 to 2 years	3 to 8 years	9+ years
Specialist	6,661 (44%)	7,246 (47%)	1,382 (9%)

Specialist job openings request a strong set of technical support and basic networking skills and tools, such as software installation, help desk support, Cisco, and Hardware and Software Configuration.

Top Skills

Baseline Skills	Specialized Skills	Software and Programming Skills
Communication Skills	Information Security	Cisco
Troubleshooting	Network Security	LINUX
Organizational Skills	Technical Support	UNIX
Writing	Information Assurance	Transmission Control Protocol - Internet Protocol (TCP - IP)
Problem Solving	Firewalls	Virtual Private Networking (VPN)
Planning	Software Installation	ITIL
Detail-Oriented	System and Network Configuration	SQL
Research	Repair	Oracle
Customer Service	Cryptography	Domain Name System (DNS)
Project Management	Help Desk Support	JAVA
Microsoft Office	Wide Area Network (WAN)	Microsoft Operating Systems
Building Effective Relationships	Telecommunications	Microsoft SharePoint
Microsoft Excel	System Administration	Dynamic Host Configuration Protocol (DHCP)
Supervisory Skills	Hardware and Software Configuration	PERL
Analytical Skills	Knowledge of Personal Computers	SAP
Computer Skills	Network Hardware-Software Maintenance	McAfee
Multi-Tasking	Mathematics	Symantec Packages
Quality Assurance and Control	Printers	Microsoft Exchange
Leadership	Local Area Network (LAN)	Python
Typing	Network Engineering	Solaris

Certifications are in-demand for Specialists, and CISSP is still the most-demanded certification as with other cybersecurity job categories, but most of the in-demand certifications for Specialists are entry-level security or networking credentials such as Security+, Network+, and Cisco Certified Network Associate.

Top Certifications

Certification	Postings	Percent of Title Area
Certified Information Systems Security Professional (CISSP)	2,425	16%
Security+	1,941	13%
Network+ Certified	1,271	8%
Cisco Certified Network Associate	942	6%
Certified Information Systems Auditor (CISA)	923	6%
Systems Security Certified Practitioner	869	6%
Certified Information Security Manager (CISM)	743	5%
Microsoft Certified Technology Specialist (MCTS)	609	4%
Microsoft Certified Professional (MCP)	505	3%
GIAC Security Essentials	483	3%

Demand for cybersecurity Specialists is strongest in Washington, D.C., as is the case for cybersecurity roles overall. However, some smaller markets have some of the strongest concentration of Specialist openings – including Colorado Springs, Honolulu, and St. Louis.

Top Metropolitan Areas

Metro Area	Postings
Washington, D.C.	2,570
New York	558
Dallas	378
Los Angeles	369
San Francisco	366
Chicago	338
Baltimore	336
Virginia Beach	278
St. Louis	267
San Diego	266

Metro Area	Location Quotient
Washington, D.C.	7.7
Colorado Springs	5.1
Honolulu	5
Virginia Beach	3.4
Baltimore	2.3
St. Louis	1.8
San Diego	1.8
Denver	1.7
San Antonio	1.7
San Francisco	1.5

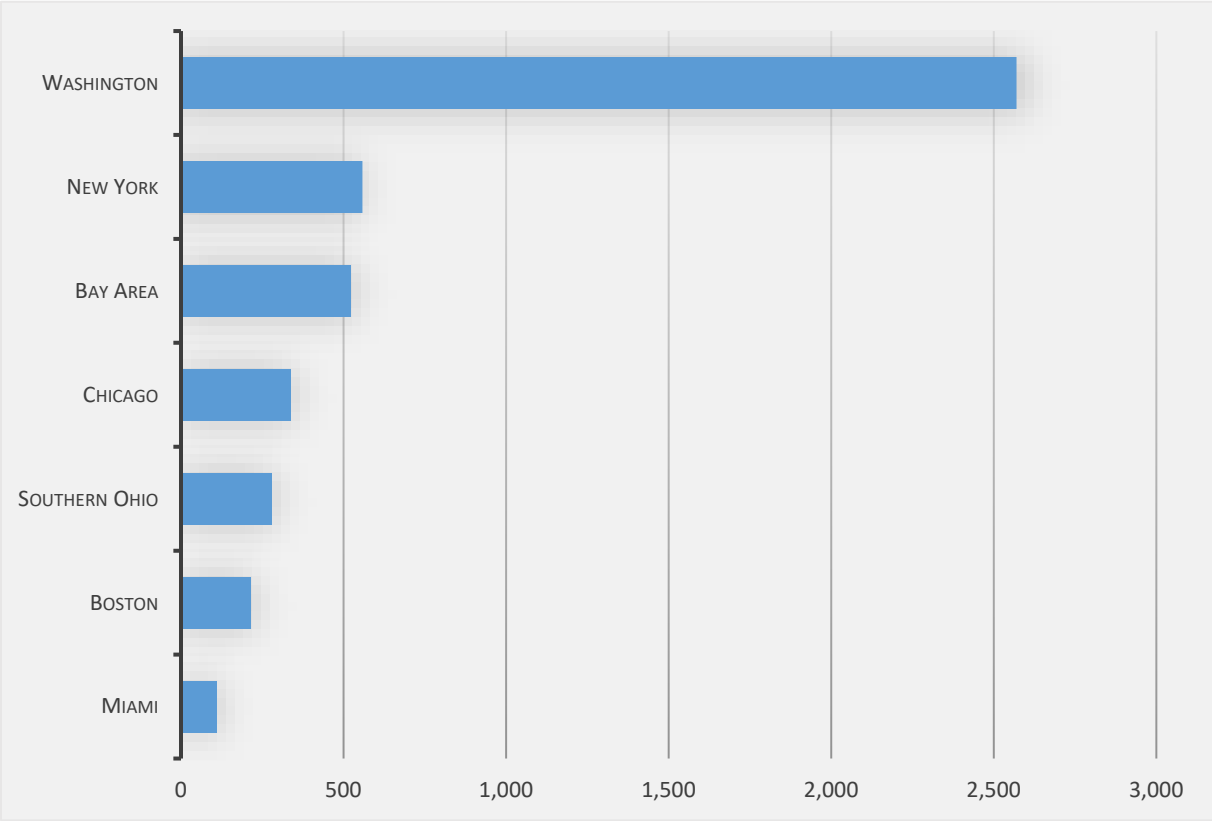
Location Analysis

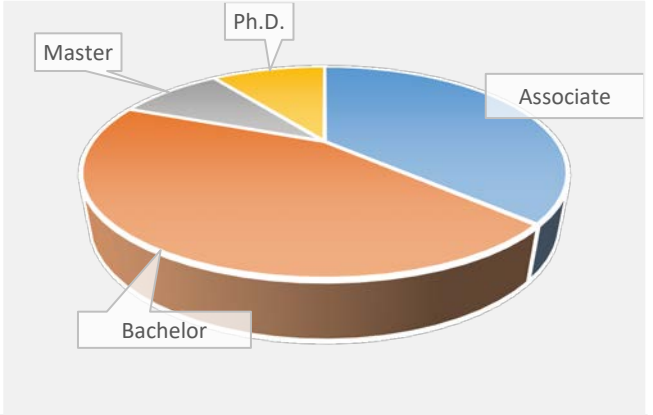
Demand dynamics for Cybersecurity Specialists differ significantly across geographies. Although demand growth for Specialists since 2010 has been strong across geographies, it ranges from 42% in Miami and New York all the way to 167% in the Bay area. Salaries also differ across geographies, from a low of $60,386 in Miami to over $100,000 in Washington, D.C. and New York. Even in the locations with heightened salaries and growth, however, Specialist jobs are remaining open for comparable or shorter lengths of time compared to the national average. This may be due, at least in part, to the combination of high salaries and low barriers to entry for cybersecurity Specialists.

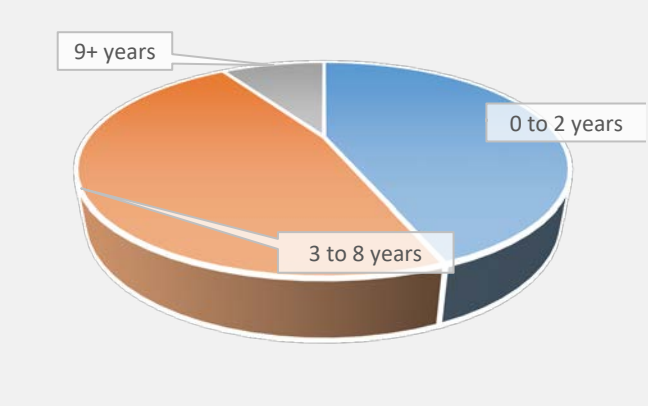
	Total Postings	Growth (2010 to 2014)	Average Salary	Average Days Open	Location Quotient
Nationally	**15,289**	**97%**	**$80,847**	**35 Days**	**1.0**
Bay Area	521	167%	$80,420	29 Days	1.5
Boston	215	60%	$88,945	21 Days	0.7
Chicago	338	132%	$83,421	35 Days	0.7
Miami	108	42%	$60,386	35 Days	0.4
New York	558	42%	$100,954	29 Days	0.6
Southern Ohio	278	136%	$75,948	25 Days	1.0
Washington, D.C.	2,570	78%	$103,994	31 Days	7.7

Across the geographies analyzed, cybersecurity Specialists have fewer sub-baccalaureate opportunities than the national average, but these opportunities are still relatively plentiful. In Boston and New York, however, only 20% and 18% of postings, respectively, are open to candidates without a four-year degree.

Job Postings for Specialists (15,289 Nationally)







	A.S.	B.S.	M.S.	Ph.D.
Nationally	**5,639 (37%)**	**6,717 (44%)**	**1,364 (9%)**	**1,569 (10%)**
Bay Area	135 (26%)	249 (48%)	65 (12%)	73 (14%)
Boston	42 (20%)	135 (63%)	26 (12%)	12 (5%)
Chicago	87 (26%)	212 (63%)	14 (4%)	25 (7%)
Miami	35 (32%)	57 (53%)	12 (11%)	4 (4%)
New York	99 (18%)	369 (66%)	69 (12%)	21 (4%)
Southern Ohio	101 (36%)	119 (43%)	42 (15%)	16 (6%)
Washington, D.C.	795 (31%)	1,334 (52%)	199 (8%)	241 (9%)

Opportunities for entry-level cybersecurity Specialists vary widely across geographies. In Boston, for example, only 21% of openings are open to workers with two or fewer years of experience; however, in Southern Ohio 54% of openings request entry-level candidates. Similarly, mid-level workers who have three to eight years of experience are requested in less than 40% of Specialist openings in both Southern Ohio and Washington, D.C., but over 60% of postings in New York and Boston request candidates with this moderate range of experience.

	0 to 2 years	3 to 8 years	9+ years
Nationally	**6,661 (44%)**	**7,246 (47%)**	**1,382 (9%)**
Bay Area	172 (33%)	309 (59%)	40 (8%)
Boston	45 (21%)	147 (68%)	23 (11%)
Chicago	129 (38%)	189 (56%)	20 (6%)
Miami	50 (46%)	49 (45%)	9 (9%)
New York	155 (28%)	341 (61%)	62 (11%)
Southern Ohio	149 (54%)	106 (38%)	22 (8%)
Washington, D.C.	1,230 (48%)	1,003 (39%)	337 (13%)

Architect

Architects oversee the design and implementation of an organization's information security systems. In 2014, there were 8,409 postings for cybersecurity Architects. They have grown in-step with the broader cybersecurity job market, with demand increasing 95% since 2010. Architects are commanding the highest salaries in the cybersecurity landscape: on average, advertised salaries for Architects are $112,659. Despite these high salaries, Architect openings are remaining open 37 days, on average – 8% shorter than cybersecurity jobs overall.

Summary Statistics

	Total Postings	Growth (2010-2014)	Average Salary	Average Days Open
Architect	8,409	95%	$112,659	37 Days

Over 80% of openings for cybersecurity Architects request workers with at least a bachelor's degree, and there is significant demand for workers with graduate degrees as well – 29% of openings request at least a master's. Although the majority of openings seek candidates with at least a four-year degree, there is also demand for sub-baccalaureate workers. Overall, 19% of openings are open to workers with less than a bachelor's degree, suggesting that some employers are willing to substitute the right mix of skills and experience for advanced educational attainment.

Educational Requirements

	A.S.	B.S.	M.S.	Ph.D.
Architect	1,617 (19%)	4,422 (53%)	1,981 (24%)	389 (5%)

Although cybersecurity Architects offer some sub-baccalaureate opportunities, the entry-level opportunities are scarce. Only 4% of openings are open to workers with two years or less of prior experience, and a third of openings request advanced workers with over eight years of work history.

Experience Requirements

	0 to 2 years	3 to 8 years	9+ years
Architect	302 (4%)	5,356 (64%)	2,751 (33%)

Architects require the same mix of core cybersecurity and networking skills common across cybersecurity roles – such as network security, firewalls, cryptography, and Cisco – but they also have strong demand for big data expertise and the requisite tools to manage both structured and unstructured datasets – such as Apache Hadoop and SQL. They also require more web-specific expertise, such as web application development, JavaScript, and XML.

Top Skills

Baseline Skills	Specialized Skills	Software and Programming Skills
Communication Skills	Information Security	Cisco
Organizational Skills	Network Security	JAVA
Writing	Firewalls	LINUX
Planning	Cryptography	SQL
Project Management	Wide Area Network (WAN)	UNIX
Problem Solving	Network Engineering	Oracle
Research	System Architecture	Virtual Private Networking (VPN)
Troubleshooting	Mentoring	Transmission Control Protocol - Internet Protocol (TCP - IP)
Presentation Skills	System and Network Configuration	ITIL
Customer Service	Business Process	JavaScript
Leadership	Web Application Development	Microsoft C#
Building Effective Relationships	HIPAA	Platform as a Service
Articulate	Systems Development Life Cycle (SDLC)	SSL
Multi-Tasking	Big Data	Apache Hadoop
Creativity	Disaster Recovery Planning	Extensible Markup Language (XML)
Change Management	Optimization	Domain Name System (DNS)
Time Management	Technical Support	Middleware
Quality Assurance and Control	Business Strategy	OSPF
Detail-Oriented	Network Administration	Agile Development

Architects have strong demand for CISSP, with 25% of openings requesting the credential. Additional certifications are also in-demand – such as CISA, CISM, and various networking credentials – but none of these certifications are requested in more than 10% of openings.

Top Certifications

Certification	Postings	Percent of Title Area
Certified Information Systems Security Professional (CISSP)	2,109	25%
Certified Information Systems Auditor (CISA)	644	8%
Certified Information Security Manager (CISM)	589	7%
Cisco Certified Network Professional (CCNP)	573	7%
Cisco Certified Internetwork Expert (CCIE)	565	7%
Cisco Certified Network Associate	444	5%
TOGAF	421	5%
Microsoft Certified Systems Engineer (MCSE)	333	4%
It Infrastructure Library	236	3%
Cisco Certified Design Professional (CCDP)	183	2%

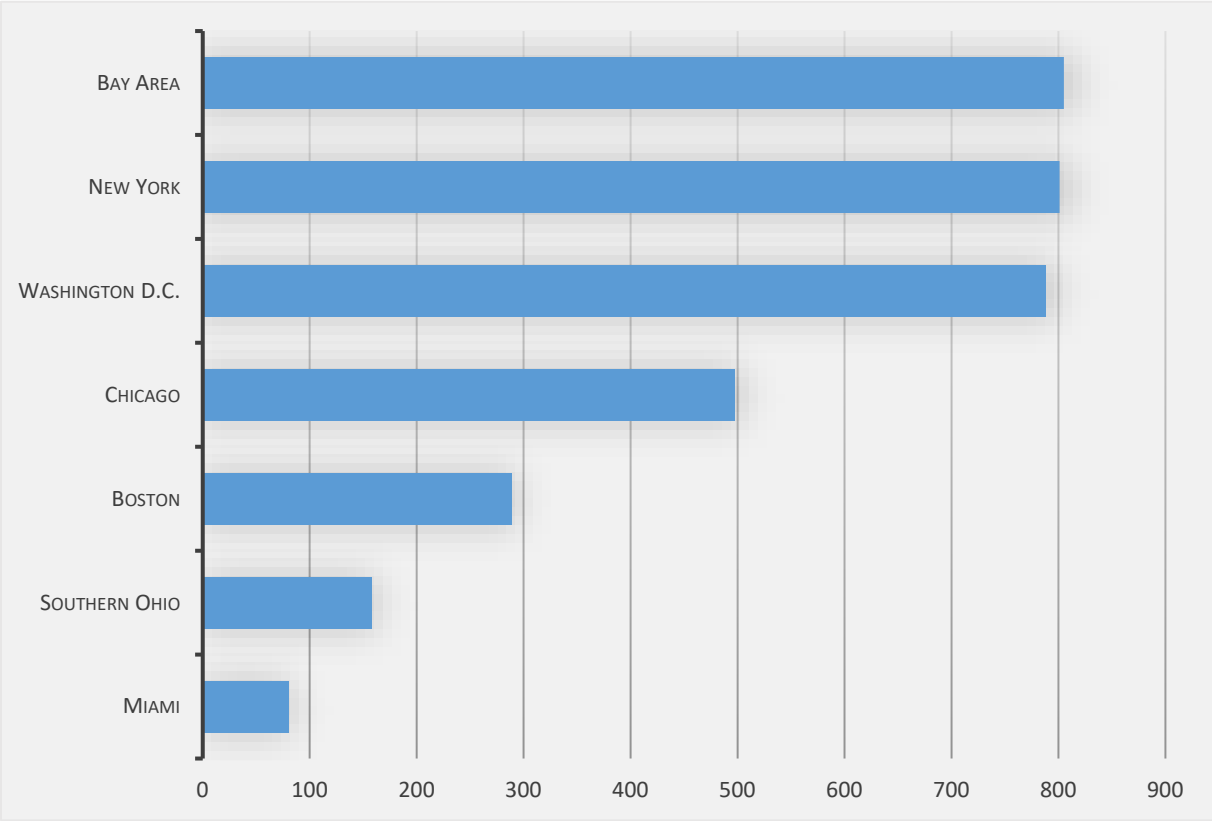
As with other cybersecurity categories, New York and Washington, D.C. have the greatest magnitude of openings for cybersecurity Architects. Unlike other cybersecurity categories, however, San Jose has the greatest concentration for cybersecurity Architects, rather than the nation's capital.

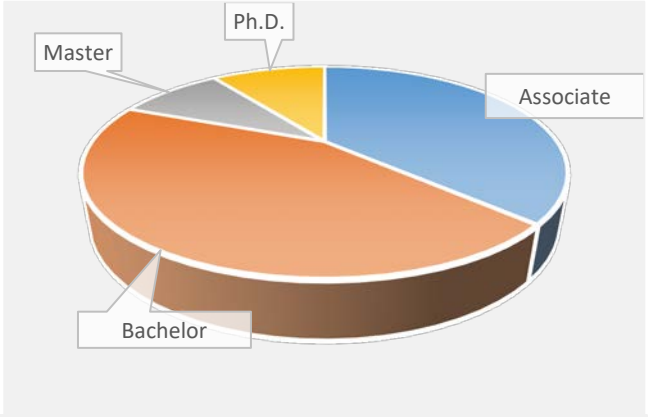
Top Metropolitan Areas

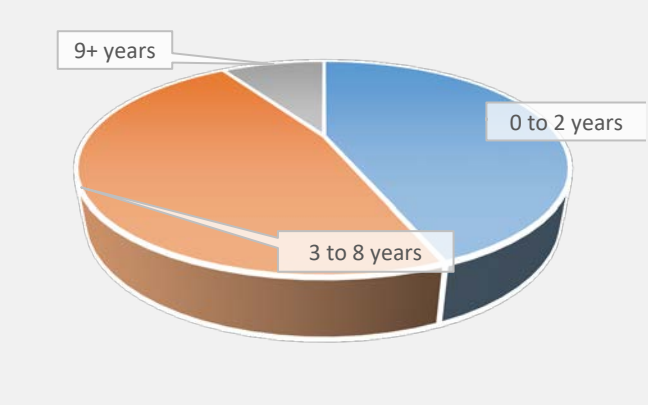
Metro Area	Postings
New York	801
Washington, D.C.	788
Chicago	497
San Jose	412
Dallas	409
San Francisco	393
Atlanta	325
Boston	289
Los Angeles	243
Phoenix	186

Metro Area	Location Quotient
San Jose	6.8
Washington, D.C.	4.3
Austin	3.0
San Francisco	3.0
Atlanta	2.2
Dallas	2.1
Chicago	1.8
Boston	1.8
Portland, OR	1.7
Denver	1.7

Job Postings for Architects (8,409 Nationally)







Location Analysis

Cybersecurity Architects consistently offer strong opportunities across geographies, although their demand dynamics vary across the key locations. Demand growth for Architects since 2010 varies from 38% in Washington, D.C. to 176% in Miami, where the concentration of Architects still has plenty of room to grow. Advertised salaries are consistently robust across geographies, in most cases pushing well into the six-figures. Posting duration does differ significantly across regions, however. In Southern Ohio and New York, openings for architects are remaining open, on average, for fewer than 30 days; in Boston and the Bay Area, by contrast, they are remaining open for 42 days – 14% longer than the national average.

	Total Postings	Growth (2010 to 2014)	Average Salary	Average Days Open	Location Quotient
Nationally	**8,409**	**95%**	**$112,659**	**37 Days**	**1.0**
Bay Area	805	120%	$136,180	42 Days	4.2
Boston	289	64%	$111,621	42 Days	1.8
Chicago	497	125%	$115,115	32 Days	1.8
Miami	80	176%	$96,944	37 Days	0.5
New York	801	100%	$125,500	29 Days	1.5
Southern Ohio	158	63%	$105,024	25 Days	1.1
Washington, D.C.	788	38%	$117,029	39 Days	4.3

This increased hiring difficulty in Boston and the Bay Area may be related to the increased educational credentials requested of cybersecurity Architects in these locations. In both cities, 88% of openings request at least a four-year degree, compared with 81% nationally. In Southern Ohio, however, nearly one-third of openings are open to workers without a bachelor's degree.

	A.S.	B.S.	M.S.	Ph.D.
Nationally	**1,617 (19%)**	**4,422 (53%)**	**1,981 (24%)**	**389 (5%)**
Bay Area	100 (12%)	393 (49%)	218 (27%)	94 (12%)
Boston	36 (12%)	153 (53%)	94 (32%)	6 (2%)
Chicago	78 (16%)	315 (63%)	98 (20%)	5 (1%)
Miami	13 (17%)	49 (62%)	16 (20%)	1 (2%)
New York	106 (13%)	439 (55%)	214 (27%)	42 (5%)
Southern Ohio	48 (30%)	80 (51%)	26 (16%)	4 (3%)
Washington, D.C.	81 (10%)	447 (57%)	208 (26%)	52 (7%)

Entry-level opportunities remain scarce across geographies: in none of the locations analyzed are more than 7% of Architect postings open to workers with two or fewer years of experience. Advanced workers are most demanded in Washington, D.C., where over 50% of openings request workers with over eight years of experience.

	0 to 2 years	3 to 8 years	9+ years
Nationally	**302 (4%)**	**5,356 (64%)**	**2,751 (33%)**
Bay Area	39 (5%)	490 (61%)	276 (34%)
Boston	13 (5%)	198 (68%)	78 (27%)
Chicago	33 (7%)	294 (59%)	170 (34%)
Miami	0 (0%)	59 (74%)	21 (26%)
New York	28 (3%)	493 (62%)	280 (35%)
Southern Ohio	4 (3%)	101 (64%)	53 (34%)
Washington, D.C.	21 (3%)	368 (47%)	399 (51%)

Auditor

Auditors conduct security audits to assess the effectiveness of an organization's information security protocols and infrastructure. They may also investigate prior breaches to understand the factors that led to a breakdown in an organization's security systems. In 2014, there were over 7,500 postings for cybersecurity Auditors, representing 132% growth since 2010 – the fastest rate of demand growth across the cybersecurity landscape. Possibly as a result of this rapid growth, Auditor postings are taking longer to fill than any other cybersecurity job category, remaining open 43 days on average. This suggests that employers are having the greatest difficulty filling these emerging roles. Despite this hiring difficulty, advertised salaries are below the average for all cybersecurity roles, though they are still in excess of $80,000.

Summary Statistics

	Total Postings	Growth (2010-2014)	Average Salary	Average Days Open
Auditor	7,533	132%	$80,750	43 Days

Auditors are among the most stringent cybersecurity job categories in terms of educational requirements, with virtually all openings demanding candidates with at least a four-year degree. In addition, 34% of openings request a graduate degree, of which 7% request a PhD.

Educational Requirements

	A.S.	B.S.	M.S.	Ph.D.
Auditor	74 (1%)	4,907 (65%)	2,055 (27%)	496 (7%)

Although Auditors are almost exclusively bachelor's-level jobs, they do offer strong entry-level opportunities. Almost one-third of Auditor job postings are open to workers with two or fewer years of experience, and only 2% of postings request workers with over eight years of experience.

Experience Requirements

	0 to 2 years	3 to 8 years	9+ years
Auditor	2,361 (31%)	5,017 (67%)	155 (2%)

Auditors are among the most hybridized cybersecurity jobs, as they require a diverse mix of auditing, risk management, business administration, data analysis, and information security expertise. These skills are rarely taught concurrently in training programs, which is likely responsible for a lack of workers possessing the skills needed for Auditor positions. This is also likely a prime driver of the heightened difficulty employers have filling these roles.

Top Skills

Baseline Skills	Specialized Skills	Software and Programming Skills
Communication Skills	Internal Auditing	Oracle
Planning	Audit Planning	SAP
Writing	Risk Assessment	UNIX
Organizational Skills	Public Accounting	Enterprise Resource Planning (ERP)
Project Management	Business Process	SQL
Microsoft Excel	Audit Reports	ITIL
Microsoft Office	Sarbanes-Oxley (SOX)	PeopleSoft
Building Effective Relationships	Audit Experience	LINUX
Problem Solving	Risk Management	Word Processing
Analytical Skills	Information Security	SAS
Presentation Skills	Business Administration	SQL Server
Research	Mainframes	Microsoft SQL
Microsoft PowerPoint	Operational Auditing	JD Edwards
Detail-Oriented	Generally accepted Accounting Principles (GAAP)	IBM Resource Access Control Facility (RACF)
Computer Skills	Sarbanes-Oxley (Sox) Audit	Visual Basic
Change Management	Management Information System (MIS)	Hyperion
Supervisory Skills	Data Analysis	Sybase
Multi-Tasking	Audit Program Development	Virtual Private Networking (VPN)
Time Management	Financial Auditing	Cisco
Microsoft Visio	Financial Reporting	Microsoft SharePoint

Cybersecurity Auditors are also among the most heavily certified positions in cybersecurity, with over 60% of openings requesting CISA certification. Over 40% of postings also request a CPA, and 21% of postings request a CISSP, which few workers are likely to have in conjunction with some of the auditing and accounting-related credentials also requested among Auditor positions.

Top Certifications

Certification	Postings	Percent of Title Area
Certified Information Systems Auditor (CISA)	4,730	63%
Certified Public Accountant	3,316	44%
Certified Information Systems Security Professional (CISSP)	1,573	21%
Certified Fraud Examiner	792	11%
Certified Internal Auditor	662	9%
Certified Information Security Manager (CISM)	627	8%
IT Infrastructure Library	184	2%
Risk And Information Systems Control	157	2%
Project Management Certification (E.G. PMP)	150	2%
Certified In The Governance Of Enterprise IT	104	1%

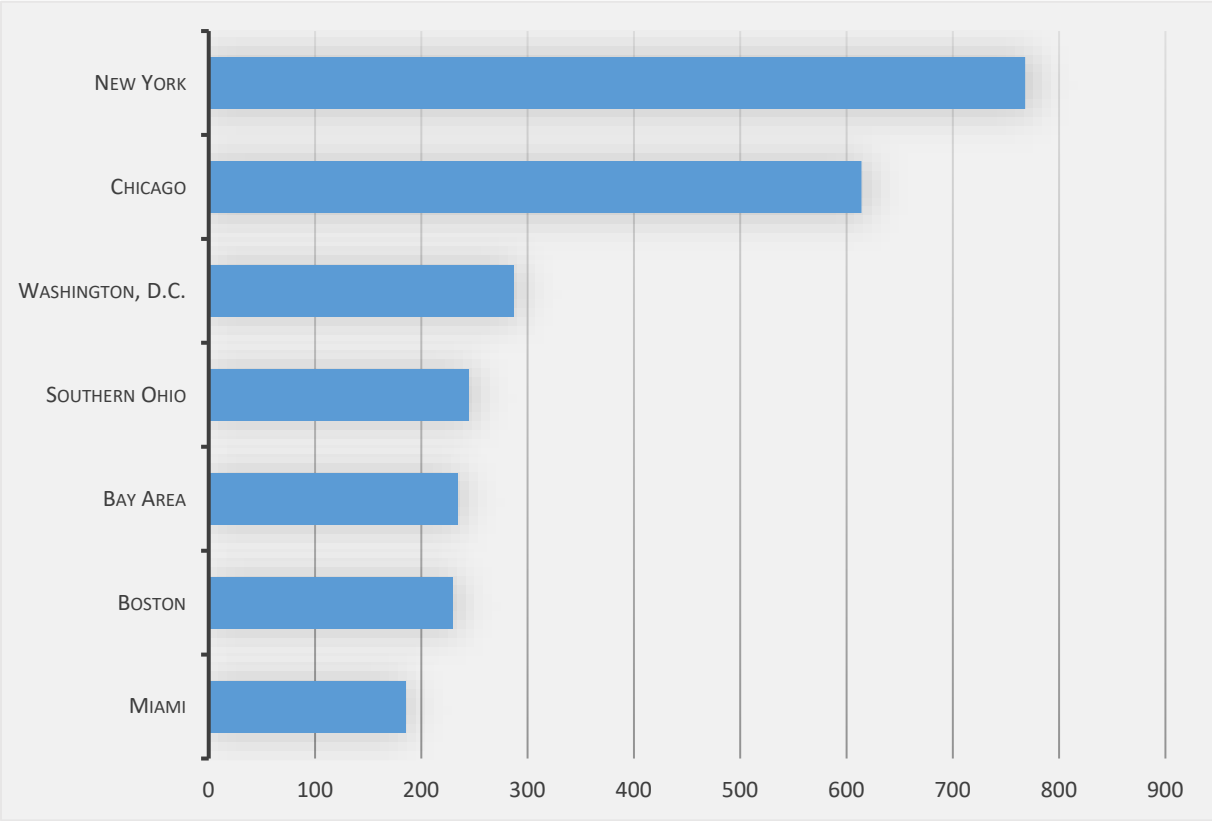
Cybersecurity auditors are most-demanded in New York, Chicago, and Atlanta, rather than Washington, D.C. or other defense and tech hubs where cybersecurity jobs are usually located. Moreover, Auditors are most heavily concentrated in finance and insurance hubs such as Bridgeport, Hartford, and Charlotte.

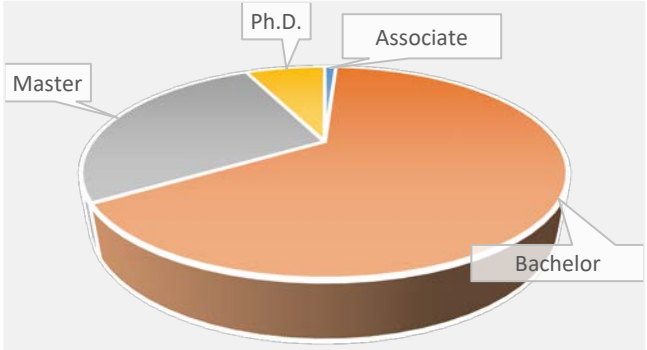
Top Metropolitan Areas

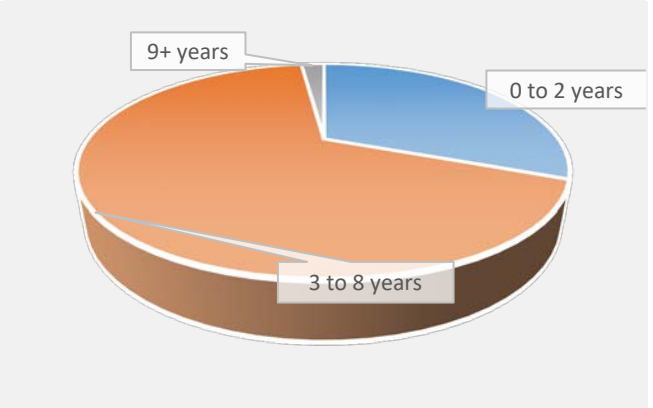
Metro Area	Postings
New York	768
Chicago	614
Atlanta	330
Dallas	291
Washington, D.C.	287
Los Angeles	231
Boston	230
Philadelphia	192
Houston	186
Miami	185

Metro Area	Location Quotient
Bridgeport	4.5
Hartford, CT	2.9
Chicago	2.5
Atlanta	2.5
Milwaukee	2.5
Richmond, VA	2.4
Cincinnati	2.1
Columbus	2.0
Charlotte	2.0
Washington, D.C.	1.7

Job Postings for Auditors (7,533 Nationally)







Location Analysis

Demand for cybersecurity Auditors has grown rapidly across key geographies, but the most dramatic growth has occurred in Chicago, Miami, and Southern Ohio. In each location, demand has surged multiple times faster than the national average. This may be a result of the main industries in these locations – which are not the traditional targets for cybersecurity of defense or technology – demanding workers to audit and improve their existing information security infrastructures. These locations also see some of the longest average posting durations for Auditors, suggesting they suffer from the greatest dearth of qualified Auditor candidates. With the exception of Southern Ohio, these fast-growing locations for Auditors also have above average advertised salaries, though they are still well below the average advertised salaries in the Bay Area, New York, and Washington, D.C., which are all in excess of $90,000.

	Total Postings	Growth (2010 to 2014)	Average Salary	Average Days Open	Location Quotient
Nationally	**7,533**	**132%**	**$80,750**	**43 Days**	**1.0**
Bay Area	234	92%	$98,332	37 Days	1.4
Boston	230	107%	$70,666	32 Days	1.6
Chicago	614	234%	$82,800	49 Days	2.5
Miami	185	340%	$81,749	48 Days	1.4
New York	768	128%	$93,800	40 Days	1.6
Southern Ohio	245	528%	$77,343	44 Days	1.8
Washington, D.C.	287	90%	$94,472	46 Days	1.7

In all locations, cybersecurity Auditors are almost exclusively bachelor's-level jobs or above, which is in-line with national norms. In Boston their educational requirements spike, with almost half of all openings requesting a graduate degree.

	A.S.	B.S.	M.S.	Ph.D.
Nationally	**74 (1%)**	**4,907 (65%)**	**2,055 (27%)**	**496 (7%)**
Bay Area	1 (<1%)	169 (72%)	50 (21%)	13 (6%)
Boston	2 (1%)	116 (50%)	58 (25%)	54 (24%)
Chicago	5 (<1%)	401 (65%)	158 (26%)	50 (8%)
Miami	1 (<1%)	119 (64%)	52 (28%)	13 (7%)
New York	8 (1%)	465 (61%)	241 (31%)	54 (7%)
Southern Ohio	4 (2%)	200 (82%)	34 (14%)	8 (3%)
Washington, D.C.	5 (2%)	222 (77%)	49 (17%)	11 (4%)

Cybersecurity Auditors also offer strong entry-level opportunities across geographies. In every location over 20% of Auditor openings seek candidates with no more than two years of experience, and in Boston over 40% of openings are open to entry-level workers.

	0 to 2 years	3 to 8 years	9+ years
Nationally	**2,361 (31%)**	**5,017 (67%)**	**155 (2%)**
Bay Area	54 (23%)	179 (76%)	1 (<1%)
Boston	93 (41%)	135 (59%)	1 (<1%)
Chicago	188 (31%)	412 (67%)	15 (2%)
Miami	60 (33%)	123 (67%)	1 (<1%)
New York	220 (29%)	534 (69%)	14 (2%)
Southern Ohio	91 (37%)	152 (62%)	1 (<1%)
Washington, D.C.	87 (30%)	184 (64%)	16 (6%)

Consultant

Consultants provide advice to inform the design and implementation of an organization's information security solutions. Consultants are the smallest cybersecurity job category in terms of total postings, as well as the slowest growing. From 2010 to 2014, demand for cybersecurity Consultants grew a relatively modest 44%. Consultants also show the least evidence of a skills gap, with postings remaining open only 31 days on average. Nonetheless, Consultant positions are still highly lucrative, advertising average salaries of $95,311.

Summary Statistics

	Total Postings	Growth (2010-2014)	Average Salary	Average Days Open
Consultant	6,294	44%	$95,311	31 Days

Although Consultant positions are lucrative, they are primarily bachelor's-level positions. Only 11% of jobs are open to workers without a bachelor's degree, and 20% of openings request graduate-level credentials.

Educational Requirements

	3A.S.	B.S.	M.S.	Ph.D.
Consultant	671 (11%)	4,388 (70%)	1,076 (17%)	158 (3%)

Despite the heightened educational requirements for Consultants, there are stronger opportunities for entry-level job seekers, with 19% of openings requesting candidates with no more than two years of previous work experience. Most of the remaining openings are seeking mid-level workers, with 69% of postings requesting workers with three to eight years of experience.

Experience Requirements

	0 to 2 years	3 to 8 years	9+ years
Consultant	1,222 (19%)	4,345 (69%)	728 (12%)

In additional to core cybersecurity and networking skills, Consultants require knowledge of risk management and risk assessment, legal compliance, and auditing. Some Consulting positions also require programming skills such as Java, C++, and Python.

Top Skills

Baseline Skills	Specialized Skills	Software and Programming Skills
Communication Skills	Information Security	UNIX
Organizational Skills	Firewalls	Oracle
Writing	Network Security	JAVA
Project Management	Business Process	LINUX
Problem Solving	Cryptography	SAP
Planning	HIPAA	SQL
Customer Service	Risk Management	Cisco
Presentation Skills	Risk Assessment	Transmission Control Protocol - Internet Protocol (TCP - IP)
Troubleshooting	Network Engineering	PERL
Research	System and Network Configuration	C++
Building Effective Relationships	Legal Compliance	Python
Microsoft Office	Sales	Virtual Private Networking (VPN)
Microsoft Excel	Internal Auditing	Enterprise Resource Planning (ERP)
Time Management	Business Development	ITIL
Analytical Skills	Sarbanes-Oxley (SOX)	McAfee
Detail-Oriented	Mentoring	Symantec Packages
English	Technical Writing - Editing	.NET Programming
Leadership	System Architecture	ArcSight
Microsoft PowerPoint	Technical Support	Tivoli
Project Planning and Development Skills	Workshops	Microsoft C#

Consultants are heavily certificated, with 32% of postings requesting a CISSP, 22% requesting a CISA, and 13% requesting a CISM.

Top Certifications

Certification	Postings	Percent of Title Area
Certified Information Systems Security Professional (CISSP)	4,730	32%
Certified Information Systems Auditor (CISA)	3,316	22%
Certified Information Security Manager (CISM)	1,573	13%
Certified Public Accountant	792	5%
Project Management Certification (E.G. PMP)	662	3%
Cisco Certified Network Associate	627	3%
GIAC Security Essentials	184	2%
Certified In Risk And Information Systems Control	157	2%
Microsoft Certified Systems Engineer (MCSE)	150	2%
IT Infrastructure Library	104	2%

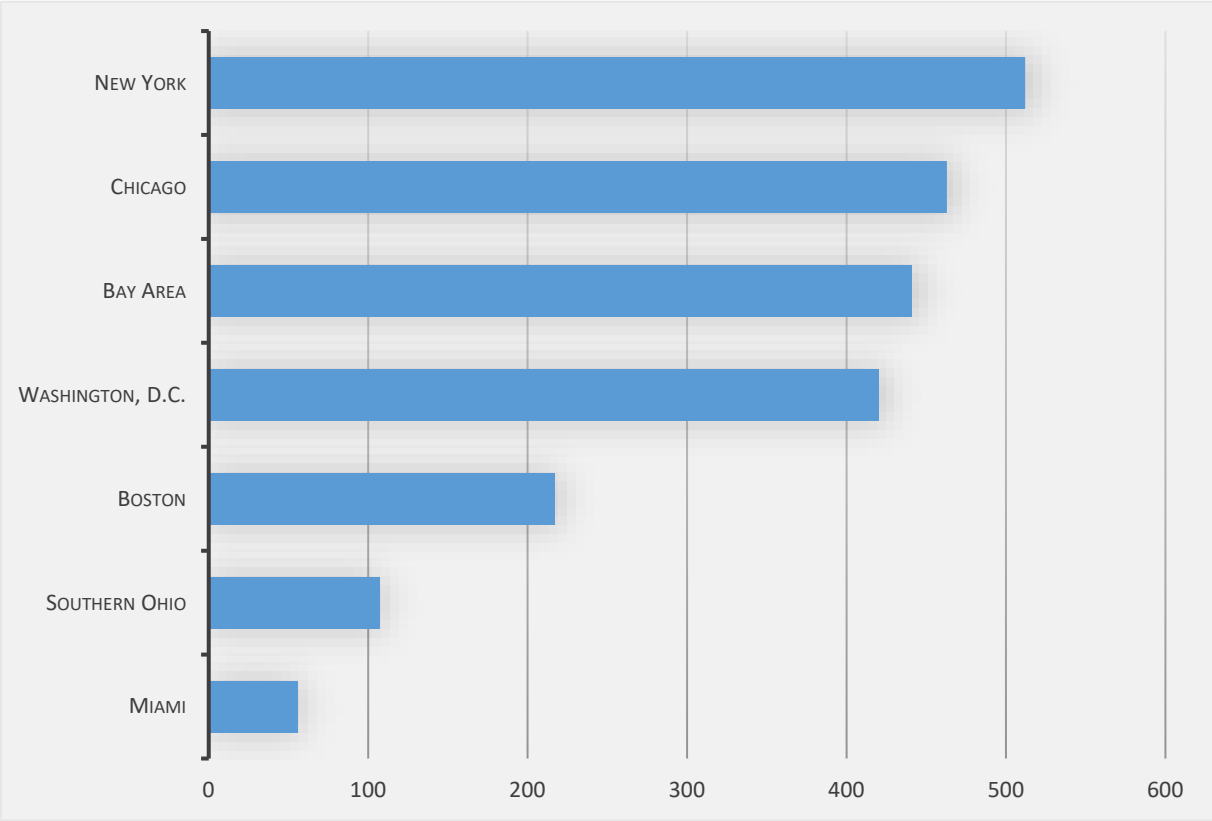
New York and Chicago are the top locations for cybersecurity Consultants, with Washington, D.C. coming in a close third. San Jose has the greatest concentration of demand for Consultants, though emerging markets for cybersecurity – such as Charlotte and Minneapolis – also show strong concentrations of openings for cybersecurity Consultants.

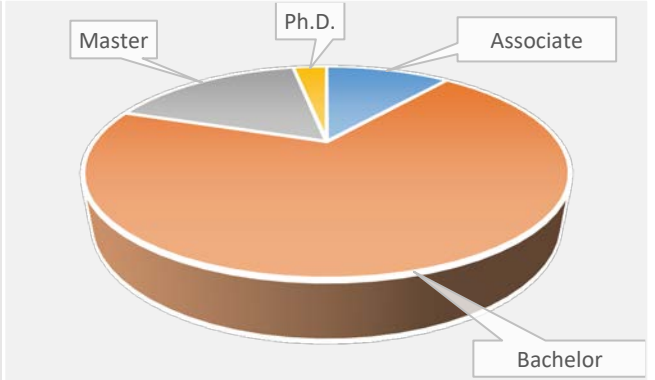
Top Metropolitan Areas

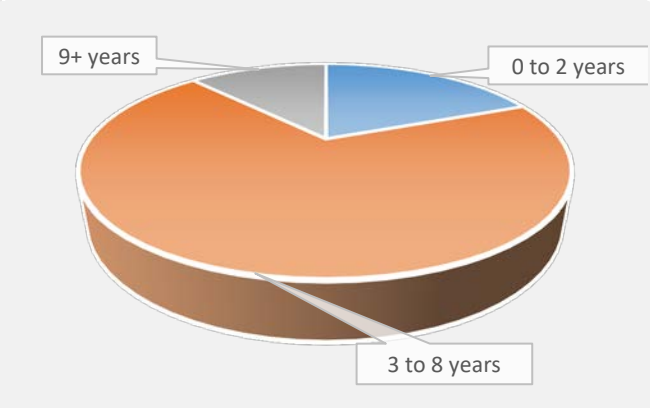
Metro Area	Postings
New York	512
Chicago	463
Washington, D.C.	420
Dallas	362
San Francisco	277
Boston	217
Atlanta	210
Los Angeles	201
Minneapolis	183
San Jose	164

Metro Area	Location Quotient
San Jose	3.6
Washington, D.C.	3.1
San Francisco	2.8
Charlotte	2.8
Dallas	2.5
Austin	2.3
Denver	2.3
Chicago	2.3
Kansas City	2.2
Minneapolis	2.2

Job Postings for Consultants (6,294 Nationally)







Location Analysis

Across the key geographies, demand growth for Consultants has fluctuated between 123% in Chicago to a decrease of 27% in Washington, D.C. Salaries also vary widely, ranging from about $75,000 in Miami to over $115,000 in Boston and Southern Ohio. Average posting durations are consistently below the overall average for cybersecurity, although they are considerably longer than the overall average for Consultants in Chicago and the Bay Area – in each city, Consultant job postings remain open for 39 days on average.

	Total Postings	Growth (2010 to 2014)	Average Salary	Average Days Open	Location Quotient
Nationally	**6,294**	**44%**	**$95,311**	**31 Days**	**1.0**
Bay Area	441	74%	$96,680	39 Days	3.1
Boston	217	113%	$116,409	33 Days	1.8
Chicago	463	123%	$102,315	39 Days	2.3
Miami	56	40%	$75,263	36 Days	0.5
New York	512	21%	$92,135	29 Days	1.3
Southern Ohio	107	51%	$117,198	24 Days	1.0
Washington, D.C.	420	-27%	$111,330	32 Days	3.1

Opportunities for Consultants consistently require, at minimum, a bachelor's degree across geographies. In every location except Southern Ohio fewer than 10% of openings call for candidates with less than a four-year degree.

	A.S.	B.S.	M.S.	Ph.D.
Nationally	**671 (11%)**	**4,388 (70%)**	**1,076 (17%)**	**158 (3%)**
Bay Area	26 (6%)	342 (78%)	61 (14%)	11 (3%)
Boston	19 (9%)	153 (71%)	39 (18%)	6 (3%)
Chicago	19 (4%)	364 (79%)	72 (16%)	8 (2%)
Miami	2 (3%)	42 (76%)	12 (22%)	0 (0%)
New York	25 (5%)	355 (69%)	117 (23%)	14 (3%)
Southern Ohio	13 (12%)	69 (65%)	24 (23%)	0 (0%)
Washington, D.C.	33 (8%)	296 (71%)	65 (15%)	26 (6%)

Consultants are primarily experienced-level roles – over 75% of Consultant postings in each location require at least three years of work experience – but entry-level opportunities vary widely. In Miami and Southern Ohio, only 8% of Consultant openings are entry-level; in Chicago and New York, however, almost 25% of postings request entry-level candidates.

	0 to 2 years	3 to 8 years	9+ years
Nationally	**1,222 (19%)**	**4,345 (69%)**	**728 (12%)**
Bay Area	70 (16%)	312 (71%)	59 (13%)
Boston	42 (19%)	155 (71%)	20 (9%)
Chicago	107 (23%)	314 (68%)	41 (9%)
Miami	5 (8%)	47 (84%)	5 (8%)
New York	121 (24%)	335 (65%)	56 (11%)
Southern Ohio	8 (8%)	87 (81%)	12 (11%)
Washington, D.C.	79 (19%)	281 (67%)	60 (14%)

REGIONAL ANALYSIS

Bay Area

	Total Postings	Growth (2010-2014)	Average Salary	Average Days Open
Overall	**13,869**	**88%**	**$117,026**	**42 Days**
Engineer	3,749	61%	$115,418	39 Days
Manager	1,666	65%	$100,304	40 Days
Analyst	1,073	126%	$94,886	42 Days
Specialist	521	167%	$80,420	29 Days
Architect	805	120%	$136,180	42 Days
Auditor	234	92%	$98,332	37 Days
Consultant	441	74%	$96,680	39 Days

Boston

	Total Postings	Growth (2010-2014)	Average Salary	Average Days Open
Overall	**6,918**	**99%**	**$104,384**	**40 Days**
Engineer	1,608	97%	$102,920	45 Days
Manager	872	67%	$103,302	37 Days
Analyst	658	147%	$89,381	35 Days
Specialist	215	60%	$88,945	21 Days
Architect	289	64%	$111,621	42 Days
Auditor	230	107%	$70,666	32 Days
Consultant	217	113%	$116,409	33 Days

Chicago

	Total Postings	Growth (2010-2014)	Average Salary	Average Days Open
Overall	**9,623**	**164%**	**$102,301**	**41 Days**
Engineer	1,527	143%	$103,993	39 Days
Manager	1,210	145%	$106,640	41 Days
Analyst	1,068	286%	$86,885	39 Days
Specialist	338	132%	$83,421	35 Days
Architect	497	125%	$115,115	32 Days
Auditor	614	234%	$82,800	49 Days
Consultant	463	123%	$102,315	39 Days

Miami

	Total Postings	Growth (2010-2014)	Average Salary	Average Days Open
Overall	**2,872**	**158%**	**$93,050**	**39 Days**
Engineer	532	173%	$87,975	34 Days
Manager	461	152%	$96,239	43 Days
Analyst	399	146%	$67,732	37 Days
Specialist	108	42%	$60,386	35 Days
Architect	80	176%	$96,944	37 Days
Auditor	185	340%	$81,749	48 Days
Consultant	56	40%	$75,263	36 Days

New York

	Total Postings	Growth (2010-2014)	Average Salary	Average Days Open
Overall	**17,982**	**90%**	**$111,202**	**36 Days**
Engineer	2,778	89%	$107,440	34 Days
Manager	2,468	81%	$108,481	37 Days
Analyst	1,853	72%	$101,241	36 Days
Specialist	558	42%	$100,954	29 Days
Architect	801	100%	$125,500	29 Days
Auditor	768	128%	$93,800	40 Days
Consultant	512	21%	$92,135	29 Days

Southern Ohio

	Total Postings	Growth (2010-2014)	Average Salary	Average Days Open
Overall	**3,908**	**151%**	**$84,257**	**31 Days**
Engineer	533	118%	$91,393	29 Days
Manager	449	94%	$79,183	27 Days
Analyst	507	137%	$67,900	33 Days
Specialist	278	136%	$75,948	25 Days
Architect	158	63%	$105,024	25 Days
Auditor	245	528%	$77,343	44 Days
Consultant	107	51%	$117,198	24 Days

Washington, D.C.

	Total Postings	Growth (2010-2014)	Average Salary	Average Days Open
Overall	**27,246**	**39%**	**$108,908**	**37 Days**
Engineer	5,793	13%	$101,233	37 Days
Manager	3,094	47%	$98,282	37 Days
Analyst	2,817	7%	$94,387	37 Days
Specialist	2,570	78%	$103,994	31 Days
Architect	788	38%	$117,029	39 Days
Auditor	287	90%	$94,472	46 Days
Consultant	420	-27%	$111,330	32 Days

ACKNOWLEDGEMNTS

We would like to express our gratitude to the individuals and organizations that have made this report possible.

First, we want to thank Burning Glass Technologies for their commitment and contributions to this research. In particular, we are grateful for the leadership of Will Markow and the analysis, insights, and commentary of Josh Konieczny and Matej Mavricek. Their selection of the appropriate data to include in this report demonstrated a real understanding of the career issues facing our young college graduates.

We are especially thankful for the direction, guidance and support of BATEC's National Visiting Committee and the contributions of BATEC's Academic Partners. Together, this collaborative group of engaged professionals bring heart, meaning and substance to the issues of Technical Education.

There are many who have contributed their ideas and input throughout this research project. That said, all errors, omissions, and views remain the responsibility of the authors.

About BATEC

www.batec.org

BATEC (Broadening Advanced Technological Education Connections), a National Science Foundation-funded Center of Excellence for Computing and Information Technologies, is dedicated to the complex mission of developing career-focused pathways and practical work experience for motivated, typically underserved high school, community college and university students in urban environments which feature a high demand for skilled labor.

About Burning Glass

www.burning-glass.com

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. 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.

About NSF

www.nsf.gov

The National Science Foundation's (NSF) Advanced Technological Education (ATE) program seeks to improve the education of technicians who work in advanced industries that are important to the nation's economy and security. The program involves partnerships between academic institutions and industry to promote improvement in the education of science and engineering technicians at the undergraduate and secondary school levels. The ATE program supports curriculum development; professional development of college

faculty and secondary school teachers; career pathways to two-year colleges from secondary schools and from two-year colleges to four-year institutions; and other activities.

This report was prepared with support from the National Science Foundation under grant DUE-110415 to the University of Massachusetts. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the editor and the principal investigators of the BATEC ATE Center. They do not necessarily reflect the views of the National Science Foundation.

BATEC

National Center of Excellence for Computing and Information Technologies
Headquartered at University of Massachusetts Boston
www.batec.org

- College and Career Pathways
- Employability and Problem-Solving Skills
- Internship Opportunities
- Industry Trends and Workforce Needs
- Education, Business, and Community Connections

Serving Boston, Chicago, Las Vegas, and San Francisco

UMASS BOSTON

COLLEGE OF ADVANCING AND PROFESSIONAL STUDIES
UNIVERSITY OF MASSACHUSETTS BOSTON

UMass Boston is a public research university with a dynamic culture of teaching and learning, and a special commitment to urban and global engagement. BATEC is headquartered in the College of Advancing and Professional Studies (CAPS) at UMass Boston, offering an opportunity to address the workforce and community needs of our regions.

UMASS BOSTON