Everything You Need to Know About a Career in Cyber Security

Including the Best Jobs in the Field and How to Land Them

Table of Contents

Everything You Need to Know About a Career in Cyber Security

Including the Best Jobs in the Field and How to Land Them

Introduction

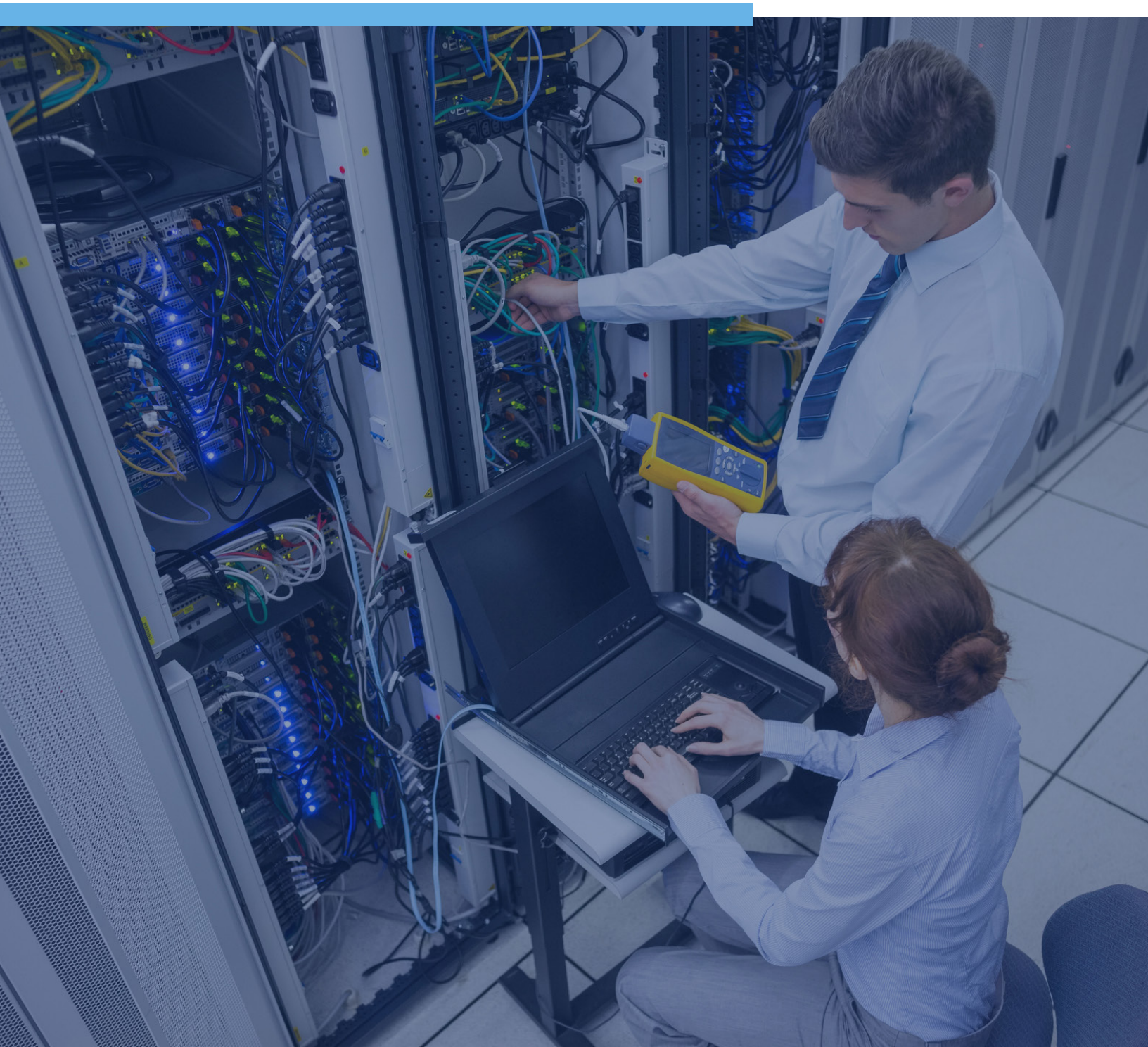
Cyber crime costs the global economy over $400 billion each year. Over the last few years there has been an increase in attacks with some of the largest companies in the world falling victim to cyber crime, including J.P. Morgan, Target and The Home Depot among others. As cyber attacks continue to increase in volume and tenacity with ever-changing tactics, the government and the private sector are raising the alarm. In response, there has been a sharp uptick in the need for cyber security professionals across almost every sector.

Today, demand in the cyber security job market is soaring while supply is running critically low. According to Cisco, there are currently one million unfilled cyber security jobs worldwide. In the U.S. alone, job postings are up 74% over the past five years with 209,000 current job vacancies, as reported by Forbes. Quite simply, there aren't enough qualified and skilled cyber security professionals to fill the growing need.

For job seekers looking for high pay, job security and the option to work in any sector and in any state, the cyber security field is the place to be. This eBook will explain why a career in cyber security is so appealing today, discuss the best jobs in the field along with salaries, and offer advice on how to land a position in this lucrative industry.

One

Job Opportunities



If there ever was a time to enter the cyber security field, it's now.

With cyber threats and attacks continuing to increase, the demand for cyber security professionals is far outpacing the supply. Job opportunities in the cyber security field are so plentiful that unemployment hovers around zero.

Between 2010 and 2014, cyber security job postings grew 91% and the field is projected to grow by 37% over the next 10 years, adding roughly 27,400 jobs to the workforce. U.S. News & World Report listed Information Security Analyst as number eight in its list of the 25 Best Jobs of 2015. As CSO reported, just over half (51.3%) of security executives and managers surveyed in Computerworld's 2016 IT Salary Survey said they expect IT staff headcounts to increase in the coming year. Marketo CSO Jason Hoffman, says his company is currently recruiting for a Director of Information Security and he expects to "expand the security team this year, focusing on technical roles such as security architects, security engineers and security analysts." Simply put, the job outlook for those entering the cyber security field is very, very strong.

Two

Cyber Security Salaries

Burning Glass Technologies reported in their 2015 Job Market Intelligence: Cybersecurity jobs report that cyber security workers earn on average 9% more than all other IT workers, which equates to roughly a $6,500 premium per year.

According to the U.S. Department of Labor's O*NET OnLine, the median annual wages for cyber security professionals range from $70,000 to $118,000. And due to the high demand for cyber security professionals, salaries are rising. "In our survey 49% of respondents make $100,000 or more—mostly attributed to those with management roles, while the largest single group (23%) selected the $80,000–$99,999 range, representing those with administrator or engineering roles," said the SANS Institute in its Cybersecurity Professional Trends Survey. What's more, the survey concluded, "Formal education is still a key factor in salaries. Respondents with a bachelor's degree or higher again made up 75% of the sample."

Salaries in cyber security are high and they are only increasing as demand for highly educated and experienced professionals in the space soars, making it hard to deny the value of a master's degree in cyber security.

Average Salaries

MANAGEMENT ROLES

49%

$100,000 +

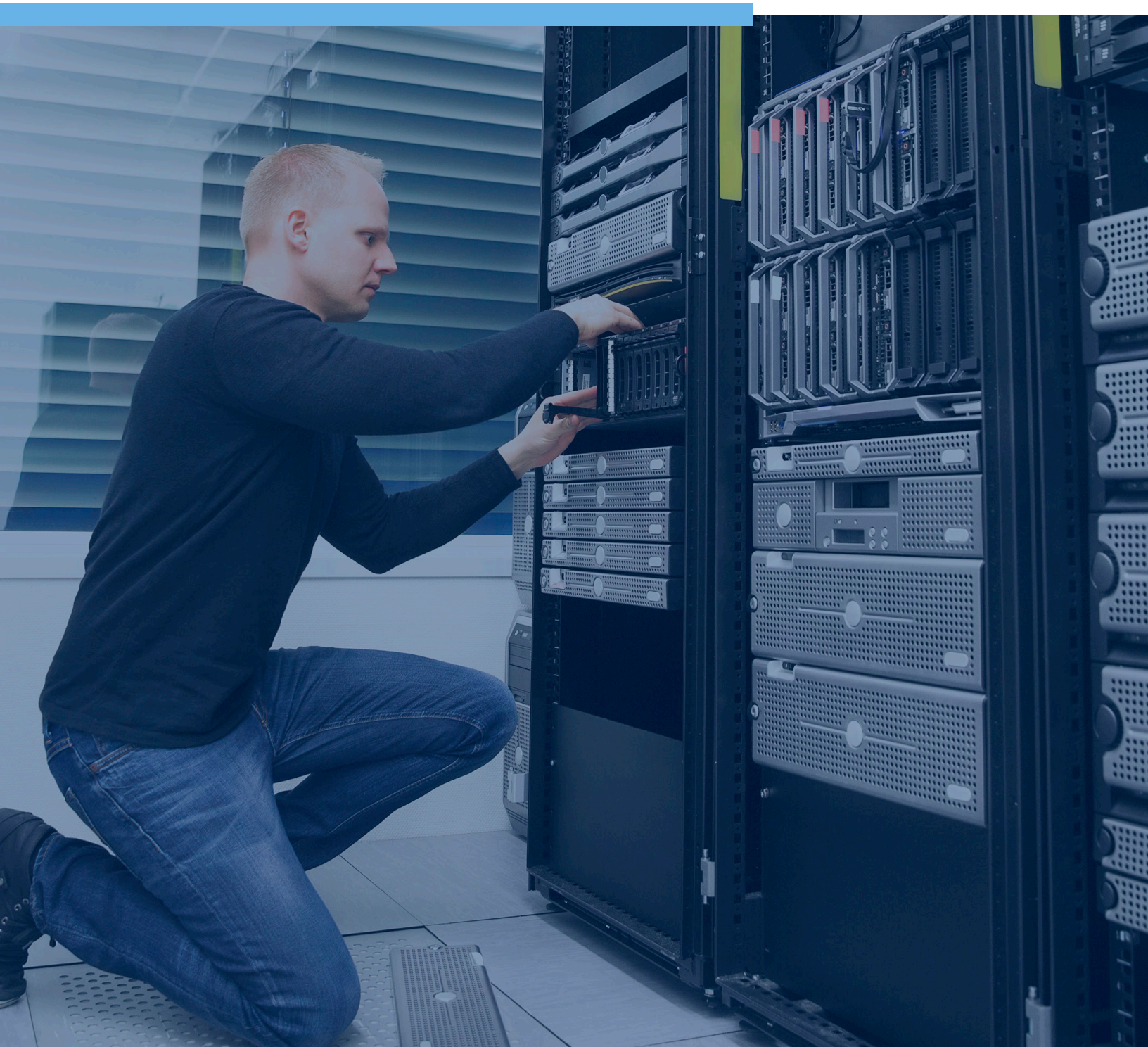
ADMINISTRATOR ROLES

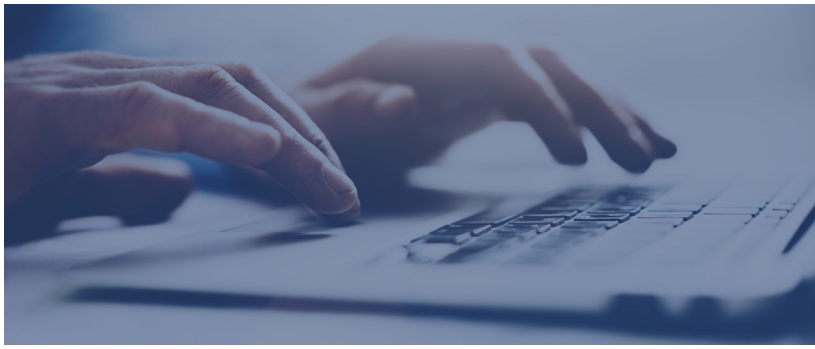
23%

$80,000 - $99,999

Three

The Best Jobs in Cyber Security





Information Security Analyst

AVERAGE ANNUAL SALARY
$49,003 – $102,219

U.S. News & World Report ranked Information Security Analyst as number three on its list of Best Technology Jobs of 2015. In this role, the main duty is to protect sensitive information. Info security analysis create the plans and implement strategies for preventing attacks, develop policies to protect the organization against such attacks, ensure compliance of policies, monitor data access and train other employees.

Lead Software Security Engineer

AVERAGE ANNUAL SALARY
$233,333

Ranked as number one on CIO's list of the 10 Highest Paying IT Security Jobs, a lead software engineer makes an average annual salary of $233,333 and is typically tasked with leading a team of security experts, analyzing and assessing risk, developing secure software and identifying vulnerabilities.

A 2015 Burning Glass jobs report found that engineering job postings accounted for 26% of all the cyber security job listings in 2014, more than any other cyber security position. According to Dice.com, cyber security engineers make up three of the top 10 best paying jobs in security:

- Cyber security engineers command an average salary of $170,000.
- Lead security engineers command an average salary of $175,000.
- Lead software security engineers command an average salary of $233,333 – more than the CSO who they likely report to.

And a Computerworld salary survey found that compensation for network engineers increased 4.6% from 2015 to 2016.

Robert Duncan, CISO of stock exchange operator Euronext N.V., said he knows of a security engineer who changed companies twice within a year and saw his salary double to about $121,000, as reported by the Wall Street Journal.

Chief Information Security Officer

The CISO is a senior-level role in charge of developing, implementing and maintaining security processes that protect the company from threats and risk.

AVERAGE ANNUAL SALARY
$192,500

Security Architect

A security architect is responsible for analyzing security threats and recommending solutions to protect information and data. They may participate in the development of security hardware and software, oversee and educate staff on security policies, design security models and install VPNs, firewalls and more.

AVERAGE ANNUAL SALARY
$81,845 – $147,873

Penetration Tester

Penetration testers are in charge of identifying vulnerabilities in an organization's network. They do this through constantly probing and testing the network using various tools and software.

AVERAGE ANNUAL SALARY
$45,192 – $120,163

Information Security Crime Investigator/ Forensics Expert

A forensics expert is a cyber crime-fighting Sherlock Holmes who investigates cyber attacks and tries to identify flaws in the system that allow for an attack by searching for clues left by the attackers.

AVERAGE ANNUAL SALARY
$55,703 – $119,079

Four

Where Are the Jobs Located?

The rise in demand has been the greatest in industries managing increasing volumes of consumer data such as Finance (+137% cyber security job growth over the last five years), Health Care (+121% cyber security job growth) and Retail Trade (+89% cyber security job growth).

Perhaps not surprisingly, California, home of Silicon Valley, the tech capital of the world, has the most cyber security job postings of any state in the United States, with 28,744 total job postings for cyber security professionals in 2014. Trailing California are Virginia, Texas, New York, Illinois, Maryland, Florida and Georgia. "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," according to Burning Glass Technologies. In addition, California and the Washington D.C./Baltimore, Maryland, area have become the leading cyber security hubs in the nation due to the national security and defense agencies that already exist there.

In San Diego, California, where some of the largest Navy and Marine bases in the nation are located, as well as the United States Navy's Space and Naval Warfare Systems Command (SPAWAR), cyber security brings more than $1.5 billion into the local economy. In response to the urgency for increased cyber security education and talent, and the growing need for collaboration between the public and private sector to fight cyber crime, the city has established a Cyber Center of Excellence (CCOE), a public-private partnership founded by a collection of world-class cyber companies with operations in San Diego.

As cyber attacks threaten the security, prosperity and privacy of the United States and its citizens, the University of San Diego realized the need to establish a Center for Cyber Security Engineering and Technology (CCSET) to address these challenges through education, training and research.

Top States for Cyber Security Jobs 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%

*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 indicated that demand is 20% more concentrated than nationally.

Five

How to Get Hired

To land a job in cyber security you must be highly qualified, which in this industry can mean years of schooling, multiple certifications and extensive experience, not to mention the right skills.

Experience

Experience in the cyber security field is invaluable. Without experience, even landing an entry-level job will be difficult. That's why it is important to take advantage of internship opportunities while obtaining your bachelor's and/or master's degree and choose a degree program that is project based, so that you are prepared for jobs upon graduation. You may also want to consider volunteering with local cyber businesses to gain real-world experience, bulk up your resume and make connections in the field.

To get hired at a higher level in the cyber security field, it is typical that employers will be looking for at least 8-10 years of experience.

Additionally, in the constantly changing field of cyber security it is imperative for cyber professionals to stay up-to-date on the latest in cyber crime. Lifelong learning, constant inquiry and vigilance are paramount for staying relevant and in demand in the cyber security field.

Education

To land a top job in cyber security, education is key. While a bachelor's degree in a related field is required for almost all cyber security positions from entry-level on up, those who aspire to the highest levels of cyber security and hope to have a long career in the profession should strongly consider a master's degree. Or if you have a bachelor's degree in an unrelated field, a master's degree is essential. Cyber security master's degree programs give students additional technical and theoretical skills, and depending on the program can offer the leadership, managerial and business skills required in high-level positions. Popular degree programs that those interested in a cyber security career often consider are:

- MS in Cyber Security Operations and Leadership
- MS in Cyber Security Engineering
- MS in Computer Science
- MS in Computer Engineering
- MS in Information Assurance
- MS in Information Technology
- MBA with a focus in cyber security

In addition, it is important to choose a degree program that will offer you the skills employers seek. In the cyber security field, technical skill is vital. When selecting a master's program make sure you look for a program that offers both a theoretical and practical foundation; one that teaches technical skill through work with real life applications.

Tips for Entry Level and Mid-to-Senior Level Job Seekers

No matter what level you are at, getting hired in cyber security depends largely on experience, what you know and who you know.

ENTRY LEVEL

Most entry-level job seekers spend months searching and networking before finding that first job. Fortunately, for those entering the field of cyber security, the opportunities are plentiful. As cyber crime becomes more rampant, the demand for cyber security professionals continues to rise. According to a recent article in Forbes, "There is a global cybersecurity labor epidemic. More than 200,000 U.S. cyber security jobs are unfilled. The cyber security workforce shortage is expected to reach 1.5 million unfilled positions by 2019."

So while there is no shortage of jobs in the cyber security field, entry-level candidates will face hurdles due to their lack of experience and education. In fact, one of the reasons for the shortage of workers in the field is not that people don't want the jobs, but that they aren't qualified.

Challenges

- Lack of practical experience and skills
- Lack of proper certifications or education (many employers look for master degree holders to fill their cyber crime positions)

Advice for Landing that First Job

- **Pick an area of focus.** Cyber security is an expansive and ever-growing field. It is important for entry-level professionals to decide what area of cyber security they want to focus on. This specialization will be appealing to employers who know that nobody, especially at the beginning of their career, can be a jack-of-all-trades. It will also help you set goals, both short term and long term, and narrow in on the jobs you are most interested in.

- **Never stop learning.** While you job hunt, work on pursuing additional educational opportunities and honing your skills. Look at what skills the jobs you are interested in require and work on acquiring those skills so that you can add them to your resume. Make a plan for how you will advance your education. Employers like to hear that a candidate has the ambition and desire to pursue higher education.

- **Network.** Networking is one of the most important things any job seeker can do. And internships are one of the best ways to network. Because internships offer you the chance to prove your skills, which is especially valuable in this very hands-on field, they can be one of the best avenues through which to gain employment upon graduation. Another way to network is to talk to people you know in the field and reach out to professionals who work in jobs that you would someday like to hold – tell them you are looking for advice and guidance as you enter the field of cyber security and would like to speak with them. Ensure you have created and updated your LinkedIn profile, and use it as a networking tool. While building professional relationships can take time, it is often one of the most effective ways to finding your first job.

- **Participate in hackathons.** Companies use places like HackerRank to view potential candidates' performance. It can be a great way to get in front of companies and demonstrate your skills.

Tips for Finding Internships

Internships, although immensely valuable, can be hard to find and as a result quite competitive once you do find them.

- **Speak to career services at your school.** Colleges and universities typically have a lot more influence with industry organizations than a single individual seeking an internship. Career services should have existing relationships with industry businesses and have built up trust, which can aid them in securing you an internship. Going after an internship in this way is a much more specialized approach than scanning job boards such as Dice.com or Indeed.com.

- **Get involved with local cyber security centers.** For example, the Center for Cyber Security Engineering and Technology at the University of San Diego is one of the only centers with an immersion program that works with a nationwide network of experts. Participation in programs like these will be greatly beneficial as you build connections and work to secure internships.
- **Seek out civic organizations in your area.** For example, the Cyber Center of Excellence in San Diego offers internships and is a great resource for those interested in the field.
- **Make yourself stand out.** This is a given. But a great resume can go a long way toward getting your foot in the door. On page 20 we offer advice on creating a resume that will get you noticed.

MID - SENIOR CAREER LEVEL

If you have already begun a career in cyber security and are looking to advance in the field, there has never been a better time to do so. Senior cyber security professionals are in high demand as companies search for candidates that have kept up with the changes in cyber security over the last decade. According to Tech Target:

> "For many years, the focus has been on perimeter defense and defending the walls of the castle," says Eddie Schwartz, the international vice president of ISACA, a nonprofit global association of 140,000 IT and information system professionals, and also chair of ISACA's Cybersecurity Task Force, as well as president and COO of WhiteOps. "The other skill set is more of a general security skill set that allows organizations to do compliance, healthcare regulations or payment card industry."
>
> The problem with both of those skill areas, according to Schwartz, is that in the last five to seven years there's been a dramatic surge in advanced threats and malware; much of it is more sophisticated than reasonable security practices and procedures driven by compliance regimes.
>
> "The emergence of security professionals that can cope with advanced threats and advanced adversaries hasn't kept up with the changes in cybersecurity," he says.

So what can you do if you find yourself in this predicament, or if you have been in the field for a while and feel you are missing certain skills that are required today? Or perhaps you have stayed current on the state of cyber security and would simply like to move up the ladder or move to a better company. No matter the case, there are things you can do to keep your resume fresh and get that next great cyber job.

Challenges

- Have not kept current on the state of cyber security
- Lack the education required to advance in your career
- Out-of-date skills
- Lack leadership skills required for advanced positions

Advice for Advancement

- **Position yourself as a leader.** This is critical if you want to move into a leadership position. Stay abreast of trends in the industry and share them with your boss and team. Offer to present at the next cyber security conference or meeting. Approach your work proactively and ensure you hone your leadership skills which includes a keen business acumen. Because leadership positions often require deep business knowledge there are degree programs specifically built for cyber security professionals looking to advance their careers and move into leadership positions.
- **Acquire necessary education.** If you have been in the field for a while you may be rusty in certain areas. If this is the case, it is critical to get up to speed on the cyber security industry today. This could include gaining certifications, advancing your education through a master's degree or taking continuing education classes.
- **Make sure you are competent in four key areas.** Hiring managers are typically looking for candidates who are strong in four critical areas: communication, risk management, technical understanding and program management.
- **Network.** Just like for entry-level job seekers, networking for higher-level job seekers is key. Beyond a professional network, social media and direct outreach, many people decide to go back to graduate school, in part, for the connections and networking opportunities higher education offers.

Certifications

If you already work in the field of cyber security, you know how important certifications are. While they are certainly not the end all be all and will not land you a job on their own, they are definite resume boosters and are sometimes required for employment. One thing to note is that while certifications may help you become a specialist in a certain area, in many cases they may not help you understand the full cyber security landscape, which is required in many mid- to senior-level roles. Important certifications that those looking to make a career in cyber security should be aware of include: :

- CISSP – The Certified Information Systems Security Professional. If you want to work at the Department of Defense, obtaining your CISSP certification is a requirement. And it carries a lot of weight beyond the Department of Defense as well. By getting your CISSP certification, you open the door to higher level positions and the possibility of increased pay.
- CISM – Certified Information Security Manager. This certification focuses on governance, risk management and compliance.
- CISA – Certified Information Systems Auditor. This certification focuses on auditing, controlling, monitoring and assessing information systems and can add a significant pay boost to a cyber security professional's annual salary.
- GIAC – Global Information Assurance Certification. This certification focuses on specialty hands-on technical capabilities such as intrusion detection and forensics among others.
- CEH – Certified Ethical Hacker. For entry-level applicants, a CEH certification can be a great way to land your first job or get you into an entry-level position at your top choice company.

Preparing Your Resume

When preparing your resume, it is essential that you make it cyber security centric. Many people applying for jobs within cyber security have a resume that may have computer science and IT work highlighted, but the cyber security aspect gets buried or left out entirely. Employers want to see exactly how your experience aligns with the cyber role they are hoping to fill. That means highlighting your depth of cyber security experience and knowledge. Explain how you have worked with varying tools, environments and protocol standards. You want to tailor your resume to the position you are applying for which means listing all the tools you are proficient with and explaining how those tools will aid you in that specific role. It is also important, however, to list your proficiency with more general tools that could apply to a wide set of jobs. Tools such as network monitoring tools, Kali Linux, Wireshark or offensive cyber tools that may be used for penetration testing, **are important to note**. Finally, be sure to highlight your accomplishments.

Once you have finalized your resume, have people you trust review it. This could include a career counselor, a professional in the field, or better yet a hiring manager.

To sum it up, when preparing your resume be sure to:

- Make sure it is cyber security centric
- Highlight your depth of experience, knowledge and education in cyber security
- Build a resume that is specifically tailored to the job you are applying for
- List the tools and software you are proficient in
- Have a hiring manager or professional in the field review your resume

Here is one example of a strong cyber security resume that successfully resulted in a job offer:

Tom Torero

Dedicated to addressing global issues through a career in the intelligence and cyber security communities.

CONTACT INFORMATION

Address: 5998 Alcala Park
San Diego, CA 92120

Phone: (619) 765-4321

Email: tom.torero@sandiego.edu

INTERESTS

- Cyber Security
- Globalization & Global Economics
- International Relations
- Foreign Languages
- Automotive Technology
- Biohacking
- Mixed Martial Arts
- Baseball
- Video Games

ACHIEVEMENTS & HONORS

- Division I Baseball All-American
- Academic All-American
- CSUN baseball team captain

Academic Experience

Cyber Security Ops & Leadership M.S. Program

University of San Diego *2016 - Present*

The knowledge and skills acquired through the USD Cyber Security Ops Masters Program are effectivly preparing me to excel in the cyber security field.

- Proficient using Kali Linux & its accompanied penetration testing tools (Nmap, Armitage, OpenVAS, etc.).
- Experience with Bash and Python scripting focused on pen testing.
- Efficient use of Wireshark (Have taken and completed Wireshark courses outside of the USD master's program).
- Able to build and configure simple networks within GNS3 Network Emulator for penetration testing.
- Actively improving proficiency in the aforementioned areas and other cyber security abilities daily.

Professional Experience

Cyber Vulnerability Analyst

Sample Company Name *2016 - 2016*

- Provide expertise in vulnerability management processes and network vulnerability scanning.
- Configure network scans, schedule network scans to run with bandwidth use in mind, and ensure accurate vulnerability assessment results are generated.
- Troubleshoot issues arising from vulnerability scanning and serve as technical expert for vulnerability assessment tools.
- Configure vulnerability assessment tools to perform vulnerability scanning on enterprise network.
- Familiarity with Netsparker Burp Suite, and other web application vulnerability assessment tools.

Education

M.S. Cyber Security Ops and Leadership (In Progress)

University of San Diego | GPA: 3.9 *2016 - Present*

M.S. in Mech. Engineering

Cal State University Northridge | GPA: 3.2 *2012 - 2013*

B.A. Sociology (Criminology Emphasis)

Cal State University Northridge | GPA: 3.5 *2007 - 2012*

Skills

Resilience

Leadership

Time Management

Goal Oriented

Communication Skills

Critical Thinking

Aptitiude

Six

Furthering Your Education

If you've decided the best path to your dream job in cyber security means that you will have to further your education, you might be wondering which degree program will be the most lucrative and appealing to employers. Oftentimes, for those in cyber security the choice comes down to a Master of Science in Cyber Security or an MBA.

An MBA

If you are considering an MBA you are likely considering one with a technical specialization. This degree can be a good option for those interested in gaining management and e-commerce skills while staying up to speed on the all-important technical side of business and the ever-growing concern over information systems security.

An MBA is the most common graduate degree in the country. This means that many, many people have found value in obtaining such an education. However, it also means that the likelihood of standing out from the crowd with an MBA is slim. If you are looking to differentiate yourself from the competition and know that you want to work in cyber security, an MBA might not give you a huge boost over fellow applicants. Plus, in order for an MBA to get you a high-level position in cyber security, you will likely need to supplement a relevant bachelor's degree and years of experience in the field with additional cyber security coursework.

On the positive side, if you want to keep your career options open and aren't ready to commit fully to a career in cyber security, an MBA offers greater flexibility because it is not as specialized (as a Master of Science in Cyber Security) and can be applied to a broad array of fields.

A Master of Science in Cyber Security

By obtaining a Master of Science in Cyber Security, you are gaining specific high-level training in a field desperate for employees with your caliber of education and experience. According to Martin Libicki, senior management scientist at RAND Corporation and lead author of the study *H4ckers5 Wanted: An Examination of the Cybersecurity Labor Market,* "The cybersecurity manpower shortage is primarily at the high end of the capability scale, commanding salaries of more than $200,000 to $250,000." This means that obtaining a master's in cyber security literally pays off. "There is a shortage of highly trained cybersecurity workers, especially in the federal government, with potential negative consequences for national security," Libicki said in a CBS News article.

The main difference, of course, between an MBA and a master's degree in cyber security is the major focus of the program – where students will spend the majority of their study time and gain the most thorough training. In a cyber security program, the focus will be on computer science and information systems, while an MBA will be primarily focused on policy, practice and business.

The Best of Both Worlds

But why should you have to choose? According to a 2015 report from Burning Glass Technologies, "The hardest-to-fill cyber security 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 the 'hybrid jobs.'"

Fortunately, you don't have to choose. If you want to combine the leadership and management aspects of an MBA with the technical, theoretical and tactical components of a cyber security degree, your best option may be a degree in Cyber Security Operations and Leadership. This degree gives you the best of both worlds by building on your bachelor's degree and your field experience to give you a deeper understating of tools and tactics for defeating adversaries, plus leadership and management skills specific to the cyber security field.

Financial Incentives, Scholarships and Grants

With cyber crime professionals in such high demand, both in the private and public sector, there are a number of financial incentives that are now being offered to those who wish to pursue a degree in cyber crime. The ICS Foundation grants a number of scholarships to those entering the field, including the graduate scholarship and the women's scholarship, which awards a full year of tuition up to $40,000. The SWSIS program offers scholarships to women entering cyber security in an effort to close the growing gender gap in the field. Two major scholarship programs are funded through the U.S. government: the Information Assurance Scholarship Program (IASP) and the National Science Foundation Scholarship for Service (SFS).

Furthermore, many employers will cover the cost of a master's degree for their employees and there are a number of programs that have been created to relieve the financial burden for veterans who wish to pursue their education.

University of San Diego

There has truly never been a better time to work in information security.

Almost every company in the world today requires experts who know how to build and protect systems to mitigate ongoing and potentially catastrophic cyber threats. If you are skilled in information security and have the education to prove it, there are immediate job opportunities all around the world, in almost every industry and across all sectors. For those who would like to make a career shift to cyber security, now could be the perfect time to make the move.

The University of San Diego offers two 21st century cyber security master's degree programs for those interested in taking their cyber security education to the next level — the on-campus Master of Science in Cyber Security Engineering and the fully online Master of Science in Cyber Security Operations and Leadership. Both programs are academically rigorous and focus entirely on modern cyber security mitigation with an emphasis on teaching students how to become effective, lifelong learners — a skill of immense importance in the ever-evolving world of cyber crime and security. If you would like to learn more about what a USD cyber security degree can do for you, contact us today.

University of San Diego

For more information on our program,

please visit our program page here or call (888) 832.0239