Getting a Degree in Cyber Security

8 Important Considerations

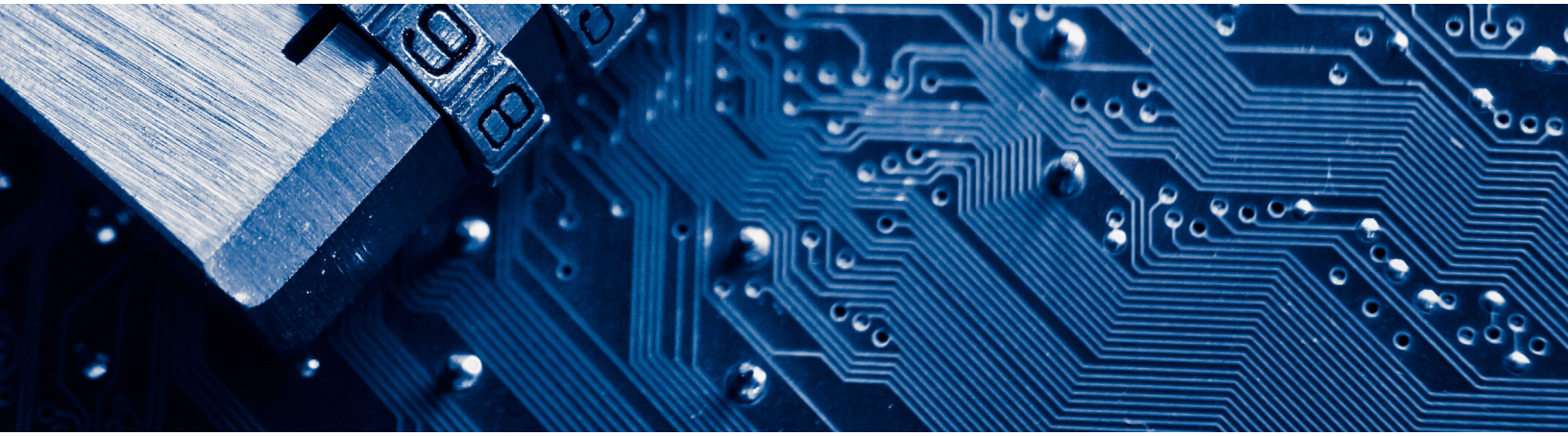
Table of Contents

Getting a Degree in Cyber Security: 8 Important Considerations

Cyber crime costs the global economy over $400 billion each year.

In 2014 some of the largest companies in the world were victims of 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 demand for cyber security professionals across almost every sector. This spike in demand has caused a severe talent shortage. And it goes beyond simply not having enough workers.



"We are not just facing a shortage of cybersecurity professionals; it is a gaping skills gap

Just over half of those surveyed (in *The State of Cybersecurity: Implications for 2015* study conducted by ISACA and the RSA Conference), or 52 percent, said that less than a quarter of applicants for cybersecurity positions have the necessary skills for the open position. As a result, 53 percent said it can take three to six months to find a qualified candidate."

- THE HILL

Similarly, a report by Burning Glass Technologies showed that

84% of cyber security postings specify at least a bachelor's degree and 23% require at least a master's. The demand for cyber security professionals is estimated to reach 6 million globally by 2019.

6 MILLION JOBS GLOBALLY BY 2019

Due to this shortage in a critical area of national security and following the law of supply and demand, those who work in cyber security can expect to earn top dollar.

For instance, on average, chief security officers will make over $220,000 annually.

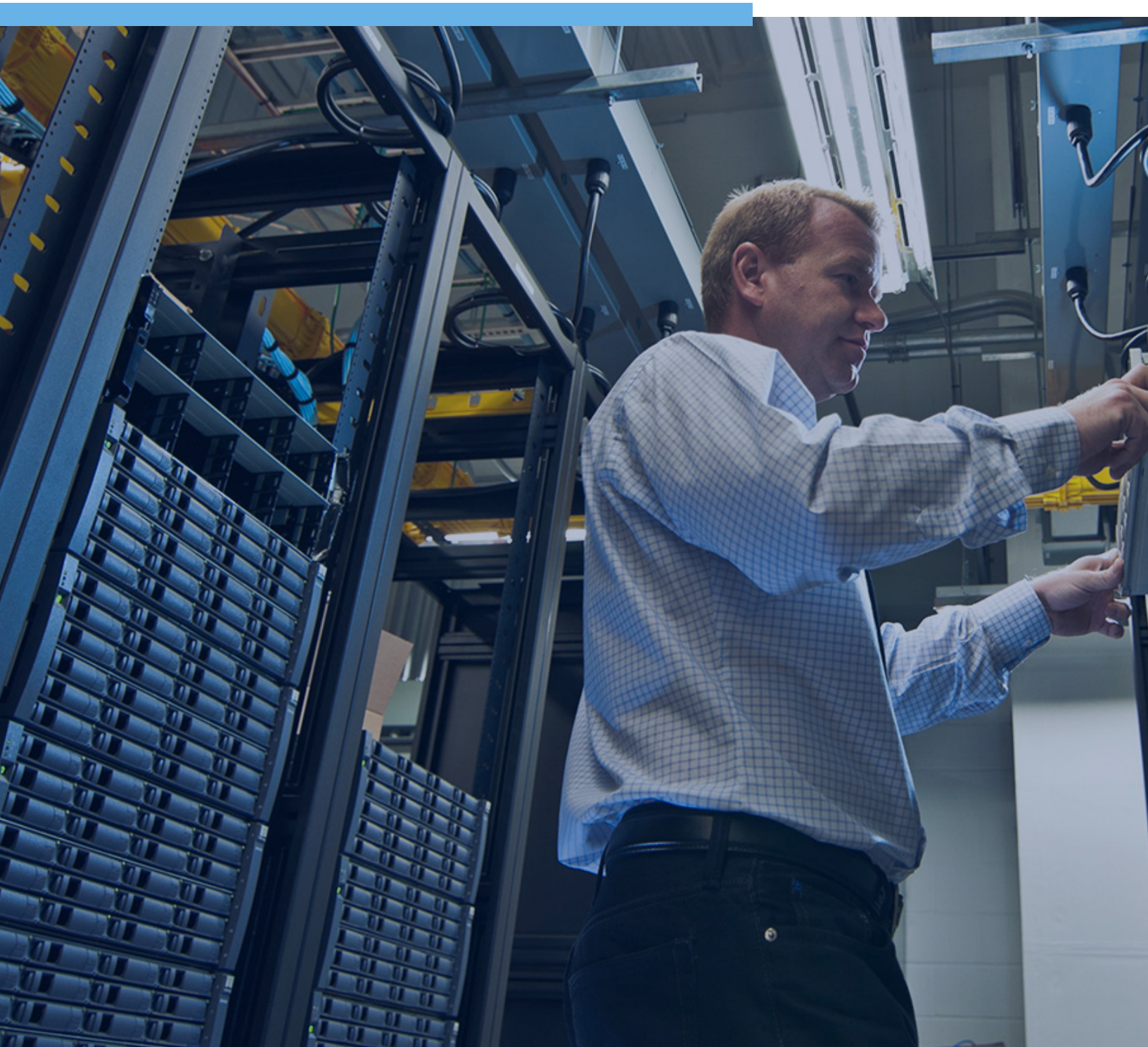
If you are considering furthering your career and are interested in a degree in cyber security, there could not be a better time to enter or advance in the field. The job outlook is fantastic, pay is prime and demand is soaring. But in order to land the best jobs in cyber security with the best companies, you need a degree. And when it comes to cyber security, the higher the degree the better.

But before you go out and enroll in a program, there are some things you need to consider.

The University of San Diego has put together a comprehensive guide for cyber security professionals looking to obtain a master's degree in the field, that covers everything you need to look for when choosing a master's program. From tuition to school reputation to the lifetime value of a degree, we've got you covered.

One

Job Outlook



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.

Between 2010 and 2014 cyber security job postings have grown 91% and the field is projected to grow by 37% over the next 10 years, adding roughly 27,400 jobs to the workforce. According to Bloomberg Business, the Pentagon plans to triple its cyber security staff by 2016 and the FBI plans to hire 1,000 agents and 1,000 analysts in the coming year.

U.S. News listed Information Security Analyst as number 8 in its list of the 25 Best Jobs of 2015. Simply put, the job outlook for those entering the cyber security field is very, very good.

Where are the Jobs Concentrated?

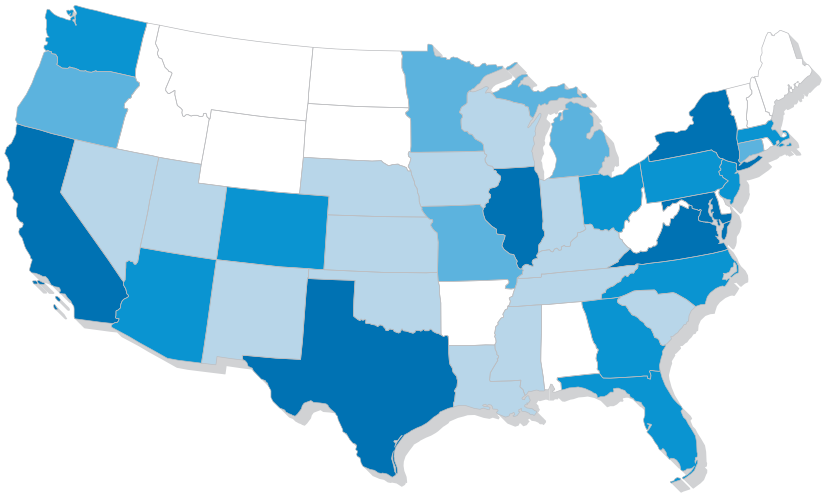
The increase in demand has been the greatest in industries managing increasing volumes of consumer data such as Finance (+137% cyber security job growth over the last five years), Health Care (+121% cyber security job growth) and Retail Trade (+89% cyber security job growth).

Perhaps not surprisingly, California, home to 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.

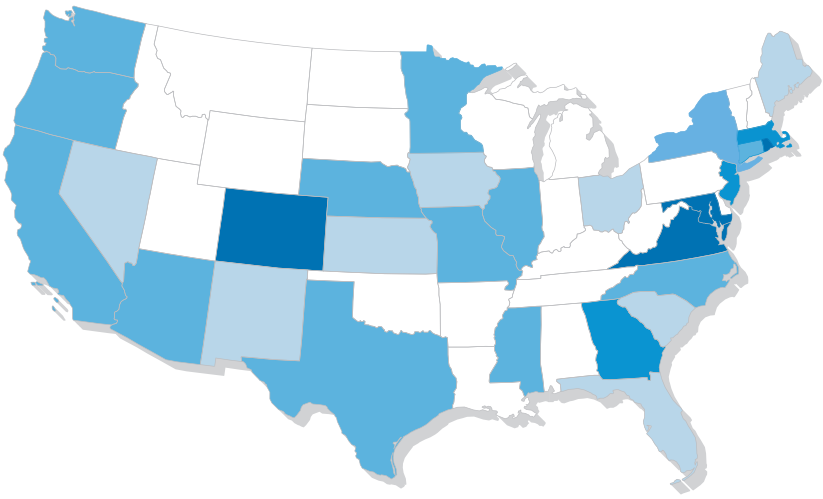
California and the Washington, D.C. / Baltimore, MD., area have become the leading cyber security hubs in the nation due to the national security and defense agencies that already exist there.

In San Diego, Calif., 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.

Cyber Security Job Postings in 2014 By State



Cyber Security Location Quotient in 2014



Top States by Total Postings*, 2014

	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 employmeny in that area. National location quotient equals 1.0; an LQ of 1.2 indicated that demand is 20% more concentrated than nationally.

©2015 BURNING GLASS TECHNOLOGIES

Two

Salaries and Career Opportunities in Cyber Security

*According to 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. Based on data from PayScale, the top five best cyber security titles, in terms of compensation are:

JOB TITLE	MEDIAN SALARY
Chief Information Security Officer	$131,322
Security Architect	$109,794
Security Director	$104,775-116,245
Security Manager	$100,215
Security Engineer	$86,996

To see specifically how much you will make based on title, years of experience, certifications and location, MeriTalk has created a Cyber Security Calculator. For example, according to the calculator:

DEPUTY CIO/CTO/CISO

- Master's Degree
- California
- 5-9 years experience

= $125,192

CYBER SECURITY MANAGER

- Master's Degree
- California
- 5-9 years

= $112,263

CYBER SECURITY MANAGER

- Master's Degree
- District of Columbia
- 1-4 years

= $109,381

When it comes to the technology sector, cyber security professionals are among the most highly compensated, posting a 9% salary premium over IT jobs in general.

And according to U.S. News, "the information security analysts that are compensated the best work in the securities and commodity contracts intermediation and brokerage industry." In terms of geography, it is in Sacramento, California; Norwich, Connecticut; and New York City that cyber security professionals make the highest salaries.

But no matter what industry you work in, if you are an experienced and educated cyber crime professional, companies want you, both in the private and public sector. And they want you today, as the severe lack of talent in the cyber crime field continues to threaten every person and business across the United States and world.

Three

Tuition

When considering a degree program, be it undergrad, graduate or doctorate, finances usually play heavily into the ultimate decision.

Tuition varies from school to school, but the total cost of a degree in cyber security will typically run anywhere from $20,000 to $40,000. Here's a snapshot of tuition at seven different schools from Massachusetts to California, as of October 2015.

SCHOOL	DEGREE	TOTAL COST
Brandeis University	Master of Science in Information Security	$32,250
University of San Diego	Master of Science in Cyber Security Operations and Leadership	$28,675
University of Washington, Bothell	Master of Science in Cyber Security Engineering	$34,830
USC Viterbi	Master of Science in Cyber Security Engineering	$37,254
University of Fairfax	Master of Science in Information Security Management (MSISM)	$32, 22
University of Maryland, Baltimore County	Master of Science in Cyber Security	Non-Resident - $32,820 Resident - $21, 330
University of Washingon, Tacoma	Master of Science in Cyber Security Operations and Leadership	$19,968

Financial Incentives, Scholarships and Grants

With cyber crime professionals in such high demand, 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 SWISS program offers scholarships to women entering the field of 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).

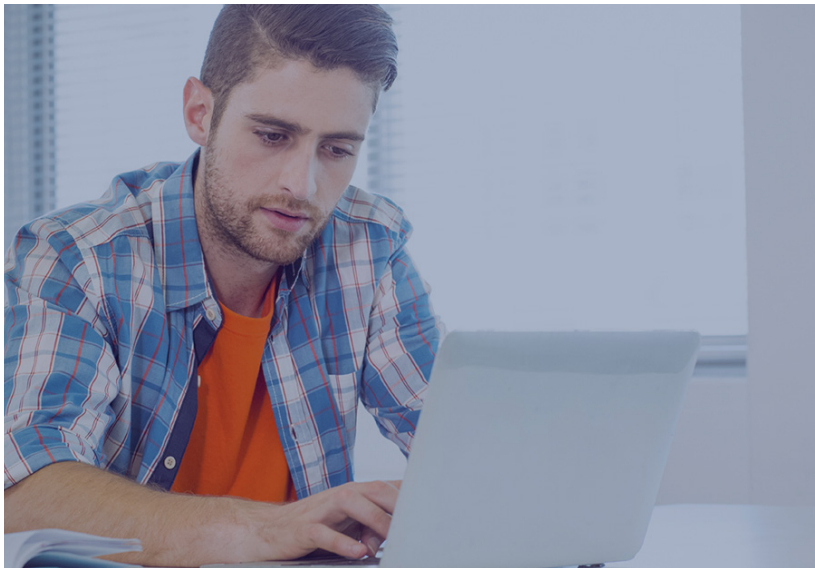
Furthermore, many employers will cover the cost of a master's degree for their employees and there are a number of programs that have been created to relieve the financial burden for veterans who wish to pursue their education.

Yellow ribbon schools, such as USD, offer support to veterans through yearly scholarship money that is then matched dollar for dollar by the VA. At USD that equals $14,896 per year.

And then of course, there are federal and state loans such as FAFSA—which help millions of students pay for higher education every year.

Four

Value of Degree Over Time



Determining the value of a master's degree and its ultimate worth is almost always the number one question every prospective student asks him or herself before taking the next step in their education.

While it's true that more education has never hurt anyone, understanding the true value of your degree in relation to how much you will have to invest to obtain that degree can help you realize the true payoff (or not) of a master's degree.

CNBC reported

"An analysis by Georgetown University's Center on Education and the Workforce found a graduate with a top-paying college major can earn an average of $3.4 million more over a lifetime than someone who graduates in the lowest-paying major. Not surprisingly, STEM majors - science, technology, engineering and math – feature prominently at the top of the pay scale."

And U.S. News reported,

"Among the 15 fields of study analyzed in the report (by the Georgetown Center on Education and the Workforce on the economic value of college areas of study), median earnings of those with a graduate degree in the field, irrespective of tenure, are an average of 38.3 percent higher than those who only possess a bachelor's degree in the same field."

Determine if Grad School is Worth it For You with the Grad School Calculator

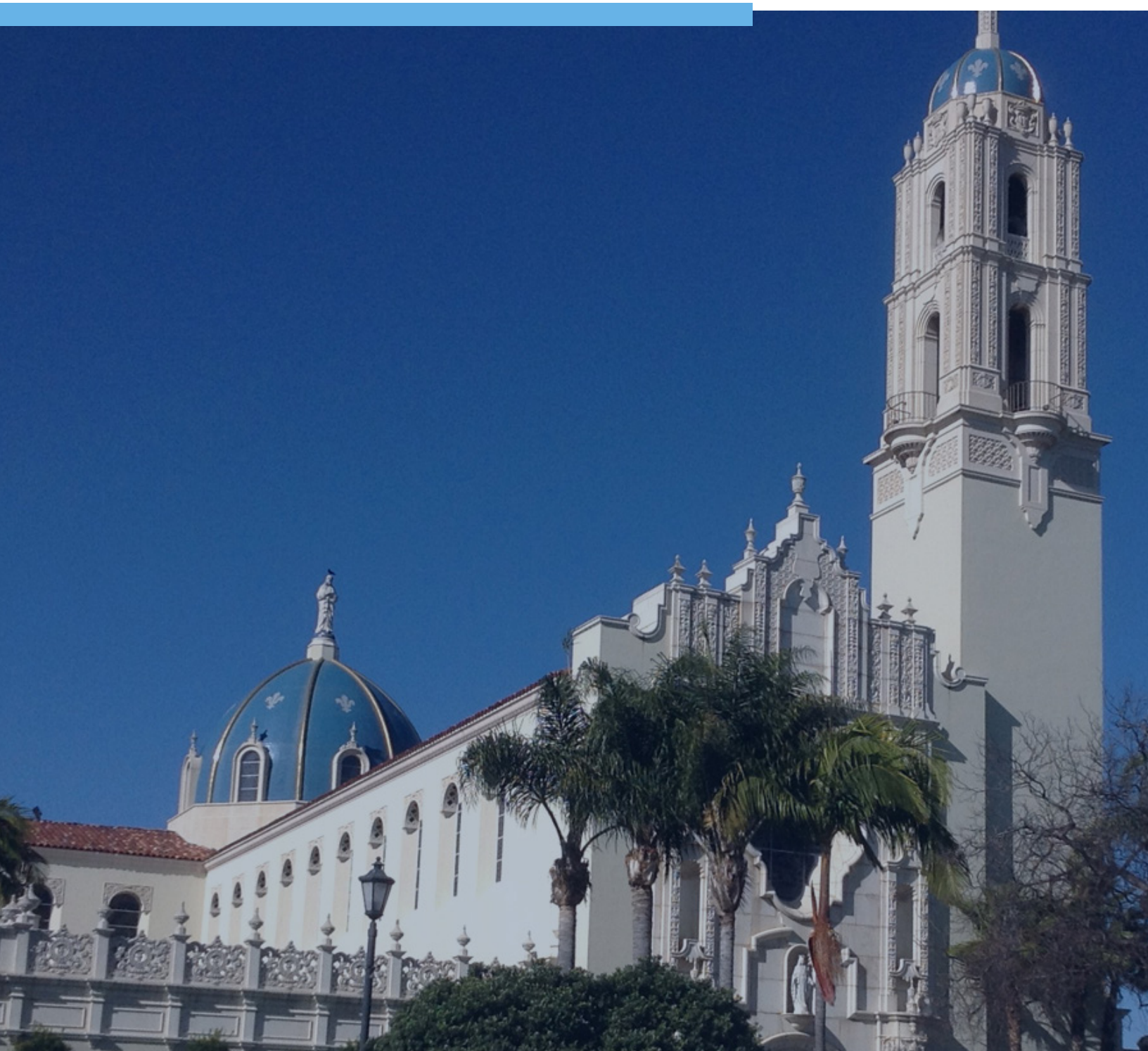
Still, while master degree holders may earn more on average, the lifetime value of a master's degree can vary greatly depending on major. This is why it's important for prospective graduate students not to rely solely on average statistics but to calculate the lifetime monetary value for themselves.

LearnVest has created a Grad School Calculator that lets you enter your earnings, tuition, loans, scholarships, retirement and additional relevant details to determine whether or not graduate school is worth it for you. In the cyber security field, where the job outlook is extremely positive, pay is high and highly educated, experienced workers are in demand, the question of whether or not a degree is worth it isn't as hard to answer as it is for someone looking to get a masters in journalism, say, where the job outlook and pay don't always pay off.

Of course, money shouldn't be the only factor when deciding upon furthering your education. But it helps to have a clear picture of the finances before making such a big commitment. Once you have a clear picture of how much you will be paying and what you will be earning in return, you can determine what you will require in terms of loans, scholarships and grants to make graduate school possible. Further, you will be able to breathe easy knowing that the tuition you are paying today will pay off handsomely in the long term.

Five

School Reputation



Reputation matters. Yet, when it comes to choosing where you will obtain your master's degree, the criteria you used for your undergrad doesn't necessarily apply.

While you want to make sure you get your degree from a university of the highest quality and caliber, it's not the overall school reputation that matters so much as the school's reputation in your field of study. In other words, the department and program reputation matters more than the school's reputation. For cyber security, the top schools aren't necessarily the traditional Ivy Leaguers you might think of.

For grad school applicants, the ability to really hone in on the schools with a strong reputation in the cyber security field is paramount. After graduation when you are applying to jobs or looking for a promotion, a department with a strong reputation in the field will be known and will carry a lot of weight.

So how do you determine what schools are the best in your field?

- If you are currently working in a related field, talk to co-workers, managers and peers to get recommendations.
- Research ranking reports such as the U.S. News and World Report.
- Reach out to former students and ask them for their feedback on the program. Sometimes colleges will provide you with this information if you ask or you can look on LinkedIn.
- Evaluate the professors in each department. Look at their background and experience, both their teaching experience and their professional experience in the field.
- Identify the top companies in your field and then look to see from which institution their cyber security experts received their master's degrees.

It is important to realize that in fields like cyber security, a constantly changing and evolving space that has exploded in recent years, many programs may be new.

But just because a program is new, doesn't mean it isn't good. It does mean that the program may not have had the time to create a reputation for itself yet. In this case, looking closely at the professors and program affiliates that may have partnered with the university to create the program can help you gauge its true caliber. And while overall school reputation should come secondary to a department or program reputation, the school's overall ranking can be a very helpful indication of a new department's strength.

Six

Choosing a Program Based on Curriculum & Objectives

Curriculum is perhaps one of the most important considerations when choosing a master's program.

Because the world of cyber security is constantly changing, it is important to seek out a master's level program that doesn't just teach skills but provides you with the tools you need to be a lifelong learner in the field. Cyber security is one of the most perishable skill sets in the world, as adversarial tactics change daily. Learning to defeat adversaries from theoretical as well as tactical perspectives, thus providing the capability to evaluate tools that can accomplish the goal of defeating threats, should be the ultimate mission of a master's level degree in cyber security, as this type of thinking and skillset is imperative for long-term success.

While every person's goals will differ, selecting a multi-disciplinary program that focuses on leadership in conjunction with cyber security strategy and management is wise when pursuing a master's degree and in light of the salary opportunities awarded at the leadership level. Far too often cyber operations or engineering specialists do not understand the "big picture" and lack the skills necessary to communicate the threat, solution or business need at multiple levels of an organizational hierarchy.

In order to gain these necessary skills and reach the highest levels of cyber security leadership, there are certain competencies that should be covered in the master's level cyber security program you choose. These include:

Cyber security strategy

Cyber security business operations — including areas such as acquisition, procurement, policy, human resources and budgeting

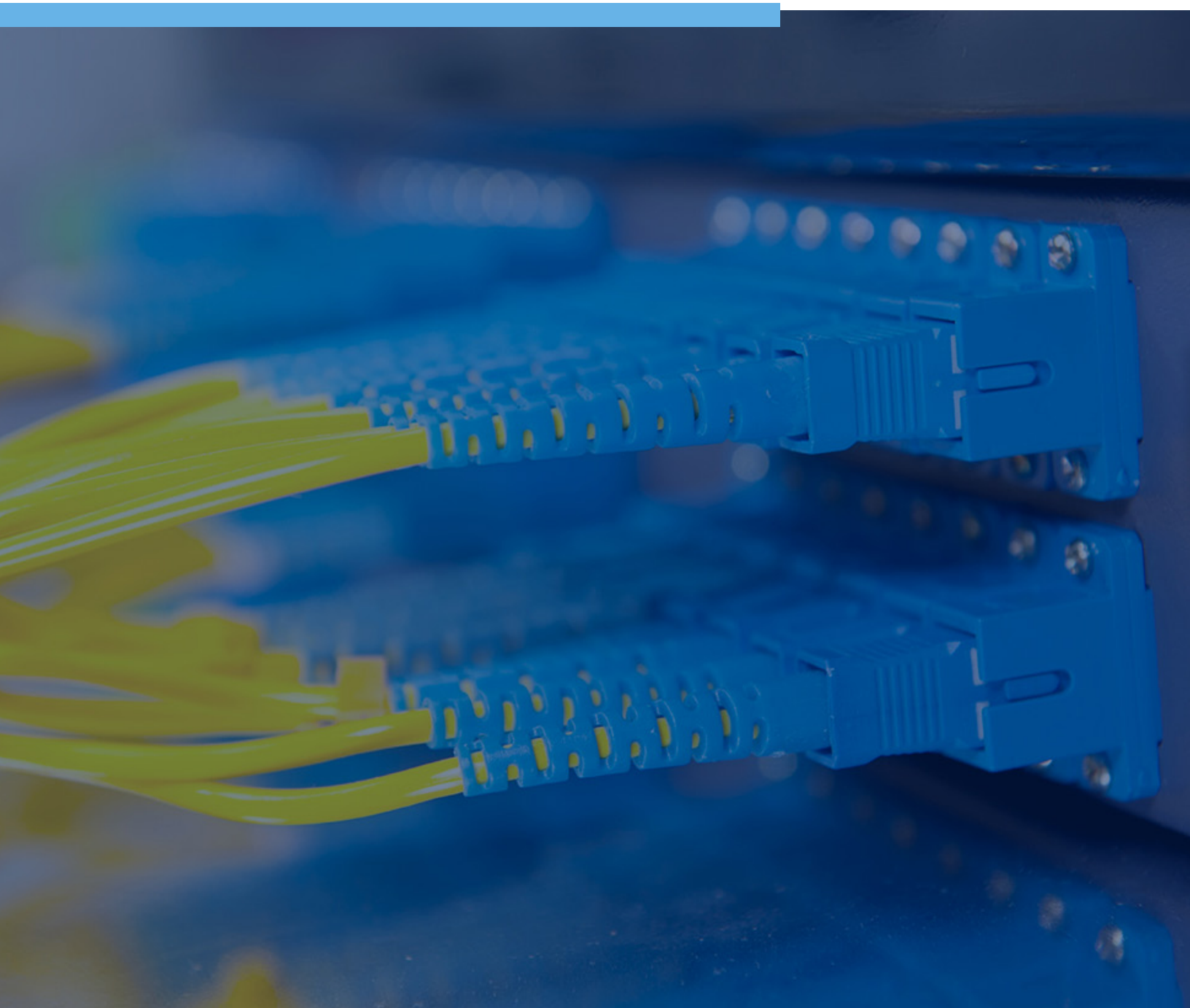
Cyber security management — including areas such as decision making, trade-offs, requirements building and team building

It is also vital to choose a program that works closely and collaborates with the greater cyber security community.

By collaborating with local and national players in the field, schools keep their curriculum current and relevant — an extremely important factor in cyber security education — and schools are able to best prepare their students for immediate job placement after graduation.

Seven

A Master's in Cyber Security vs. an MBA



So you work in cyber security or a related field and want to move up the cyber security ladder to a more prominent, better paying position.

You've decided your experience combined with a master's degree is the best path to your dream job. But what master's degree will be the most lucrative and appealing to employers? Oftentimes, for those in cyber security, the choice comes down to a masters in cyber security or an MBA. Both programs offer the managerial skills needed to work in the highest-level positions. But there are some big differences as well.

An MBA is the most common graduate degree in the country.

If you are looking to differentiate yourself from the competition and know that you want to work in cyber security, an MBA might not be the way to go. By obtaining a graduate degree in cyber security, you are receiving specific high-level training in a field desperate for employees with your caliber of education and experience. On the other hand, 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 more flexibility because it is not as focused and can be applied to a broad array of fields. In order for an MBA to get you a high level position in cyber security, however, you will likely need to supplement a relevant bachelor's degree and years of experience in the field with certain cyber security certifications.

Other degree options that you may consider are:

- MS in Computer Science
- MS in Computer Engineering
- MS in Information Assurance
- MS in Information Technology

However, if you are looking to combine the leadership and management aspects of an MBA with the technical, theoretical and tactical components of a cyber security degree, the best option may be a degree in Cyber Security Operations and Leadership.

This degree option 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.

Deciding what degree is right for you depends largely on your objectives and goals. By looking closely at what each program offers and aligning the objectives of each program with your own career and educational objectives you will be able to find the best degree path for you.

Eight

Online Vs. In Person Degree Options

Finally, for many people considering a master's level degree, flexibility is of utmost importance.

In order to balance school with a full-time career and family obligations, the option to obtain a degree online can present an opportunity that otherwise may have been impossible.

Today, many colleges and universities offer online options; either hybrid programs or in some cases 100% online degrees. And it's not just the for-profit schools that offer online degrees. Today, a number of non-profit public and private universities offer online options that are top notch and nationally ranked.

The flexibility of an online degree program offers students a number of benefits including the ability to access the best programs, professors and universities despite their physical location; pay less for materials (often times textbooks are replaced with digital content that can be viewed online or printed) and interact with students from around the country and globe. And as e-Learning Industry stated, "According to a recent study conducted by The Research Institute of America, e-Learning has the power to increase information retention rates by up to 60 percent. That means that, not only is e-Learning more cost efficient, but also it's also more effective (in terms of how much knowledge is truly acquired during the learning process)."

Plus, there couldn't be a better teaching medium for those interested in cyber security than the Internet.

As Alec Ross, senior adviser for innovation at the State Department said in a Washington Post article,

> " 'If any college student asked me what career would most assure 30 years of steady, well-paying employment, I would respond, cybersecurity.' "

Cyber security is a field with an abundance of jobs and yet not nearly enough qualified applicants to fill the slots.

And that's a concern for businesses and government alike. President Obama has requested a $14 billion budget for 2016 in order to fight cyber crime and businesses in the private sector have realized the vital importance of a dedicated cyber security team – and they're willing to pay for it. For those in the field, looking to up their qualifications and land one of the many available jobs across the country, getting a master's degree is a wise decision and one that is sure to pay dividends, indefinitely, as the world relies more and more on the Internet and technology and as cyber crime consequently intensifies.

At the University of San Diego we offer a 100% online Master of Science in Cyber Security Operations and Leadership that was developed to address the most pressing needs in cyber security today, using input from the NSA, CIA, NRO, FBI, United States Strategic Command, United States Cyber Command, United States Air Force, United States Navy, Department of Homeland Security, and many corporations, academia and relevant civic groups.

University of San Diego

For more information on our program,

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