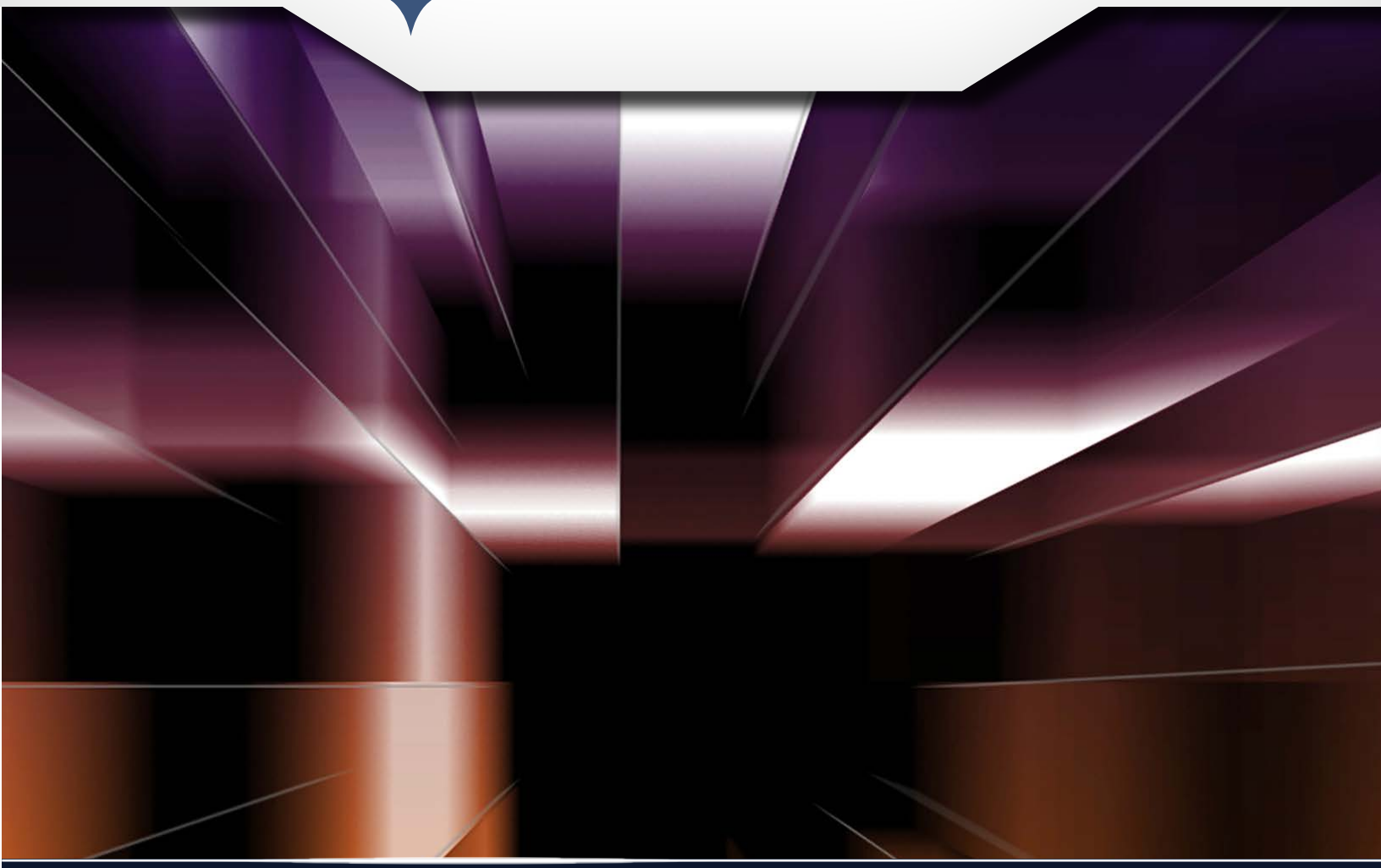
MARYMOUNT UNIVERSITY



A GUIDE TO GETTING A MASTER'S IN CYBERSECURITY

About This eBook

Demand for highly qualified cybersecurity professionals continues to grow. Recent studies by organizations such as Cisco, ISACA, and Symantec predict a cybersecurity labor shortage in the millions in the next few years.

A good master's degree in cybersecurity can lead to an outstanding career with a good salary, many job opportunities, job security, and great satisfaction in your role to protect the world (individuals, companies, government) in our increasingly digital society.

There are many programs in cybersecurity including technical degrees, certification training, and advanced degrees. Choosing among them can be challenging even for someone in the technology field. But what do you need for what type of jobs?

This eBook is designed to help you to know what to consider when evaluating different advanced-level cybersecurity programs to ensure that you are ready for the workplace whether in government or industry. This eBook also includes some tips for preparing to apply for a cybersecurity master's degree.

About Marymount University and Cybersecurity

Marymount University is a very diverse, independent Catholic institution in Arlington, VA, close to Washington D.C., a major center of cybersecurity policy, operations, and jobs. Marymount is designated by the National Security Agency (NSA) and the Department of Homeland Security (DHS) as a Center of Academic Excellence in Cyber Defense Education (CAE/CDE).

The University offers bachelor's, master's, and doctoral programs in cybersecurity. Students can take courses face-to-face or online, full or part time, all taught by world class faculty.

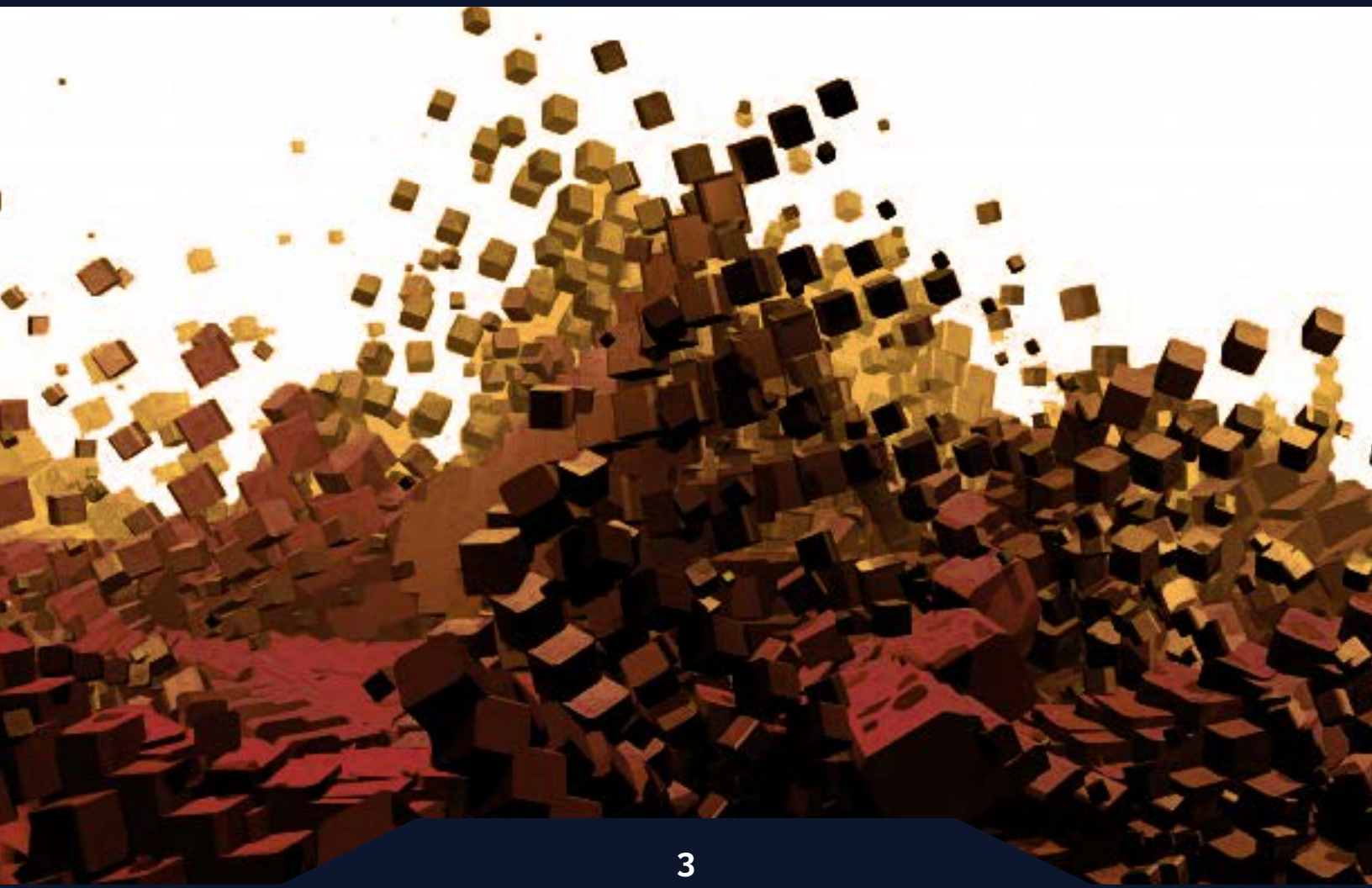
Students can do cybersecurity internships in the area and obtain good positions upon graduation within the government, government contractors, commercial companies, and not-for-profit organizations in the region.

About the Author

Dr. Diane Murphy began her career in the European pharmaceutical industry and was an early leader in chemical informatics, using technology to predict the biological and toxicological effects of chemicals. She came to the US in 1980 to use that expertise to support the U.S. Environmental Protection Agency (EPA). Later in the 1980s and 1990s, Dr. Murphy was a serial entrepreneur, founding and operating two U.S. companies (one in software development and one in corporate training), as well as a not-for-profit to help young entrepreneurs succeed in their initial technology business ventures.

In 2002, Dr. Murphy joined Marymount University as a professor of information management. Her research interests include cybersecurity education, using data science in cybersecurity, and health care security. She currently leads the university's technology programs, including cybersecurity. Dr. Murphy has many publications in the field and is an invited speaker at many cybersecurity education and workforce events.

What to Look For in a Cybersecurity Program



What to Look For in a Cybersecurity Program

Ask: Does the program cover all the aspects of cybersecurity?

Cybersecurity is an ever expanding field. It is not just network security any more. There are many jobs available in policy development, in compliance, and in security management.

Look for a cybersecurity program that offers courses that cover a range of topics necessary to work in today's cybersecurity environments. Ensure that the program teaches more than technical details; employers want candidates that can write, can work in teams, and can think critically.

Ask: Is the program accredited?

Actually, there are no cybersecurity accreditation programs at this point in time. However, make sure the university offering the cybersecurity master's degree is "regionally" accredited as this validates the overall academic environment at the university.

As is the case within Marymount, programs can be designated as a National Center of Academic Excellence in Cyber Defence Education (CAE/CDE). This designation includes a formal evaluation of all the courses in the program and their coverage of cybersecurity topics. These institutions are recommended to teach cybersecurity to prepare students for the workplace.

Ask: What credentials and experience do faculty have?

Faculty should be a combination of full-time faculty and part-time faculty working in the cybersecurity field. Full-time faculty will be available, not just to teach, but to advise you on the best options in the program to meet your individual needs and to help you find opportunities in the field. They have deep subject knowledge and are active researchers in the field. Part-time faculty bring real-world experience in the classroom and can help students reach their career goals.

Ask: What is the teaching style? Will there be any hands-on activities?

A master's degree in cybersecurity can be taught in a number of ways, but it should not be all lecture. There must be some hands-on activities and critical thinking and analysis portions.

Most master's degrees in cybersecurity will assume that you have a good knowledge of information technology on which to overlay the cybersecurity knowledge that you are learning in the same way a medical degree assumes that you have a knowledge of biology.

Look for a program that offers some hands-on activities and learning cybersecurity tools and techniques for both attack and defense scenarios. Also, be prepared to set up your own cybersecurity network and be prepared to learn and practice on your own time.

Programs that provide some hands-on opportunities better prepare you to be an effective cybersecurity professional. Programs that provide electives also allow for customization to meet individual needs and talents.

Ask: How diverse are the faculty and students?

Programs vary in the diversity, ethnic, gender, and technical expertise of the students and the faculty. Minorities and females are currently grossly underrepresented in the cybersecurity workforce, so find out about the makeup of existing programs and any initiatives they are taking to promote diversity. Faculty act as role-models, so check them out also.

Ask: What type of job can I expect upon graduation? And how does the university help me find the opportunities?

The best cybersecurity programs will prepare you for the cybersecurity workplace, whether in the public or private sector. There are so many cybersecurity jobs around the country; some may be in network defense, others may be in policy positions, others may be managing cybersecurity projects and teams, while others might be in auditing or compliance.

Graduates of the program should still be closely connected with the faculty and existing students and act as mentors, identify internships and job opportunities, and participate in program activities such as panel discussions. The university, through the program or a career center, should provide help in resume preparation and interview practice sessions. Also, ask to talk to an existing student or recent alum!

Did you know?

Over 1 million adults become cyber crime victims every day. 14 cyber crimes occur every second.

About Marymount's Cybersecurity Master's Program

Coverage of All Aspects of Cybersecurity

Marymount's 36-credit program, with both online and face-to-face options, covers both the technical and non-technical aspects of cybersecurity to meet a variety of jobs in the region. Students may also enroll in an MBA/M.S. Cybersecurity and M.S. IT/M.S. Cybersecurity dual degree programs to include other interests.

Designation and Accreditations

Marymount is designated as a Center of Academic Excellence/Cyber Defense Education (CAE/CDE). The University is regionally accredited through the Southern Association of Colleges and Schools (SACS).

Faculty Credentials

Our international faculty includes ten full-time tenure track faculty researching in many aspects of cybersecurity including machine learning, human aspects of cybersecurity, natural language processing, and data science. We also hire about 20 cybersecurity professionals each year to teach specialized courses. These professionals work in the government (FBI, Labor, DHS, for example), for government contractors (Deloitte, Northrop Grumman, for example) and commercial companies (Amazon Web Services, for example).

Teaching Style

Our faculty use a variety of teaching styles to engage students in the learning process. All our courses are taught directly by the full-time and part-time faculty: We do not use teaching assistants.

Many Marymount classes have extensive, hands-on activities and the University runs additional workshops to cover additional tools. Communication, written and verbal, is an essential component of many courses in the program. Cybersecurity is a team sport, so working in groups is extensively covered in the program.

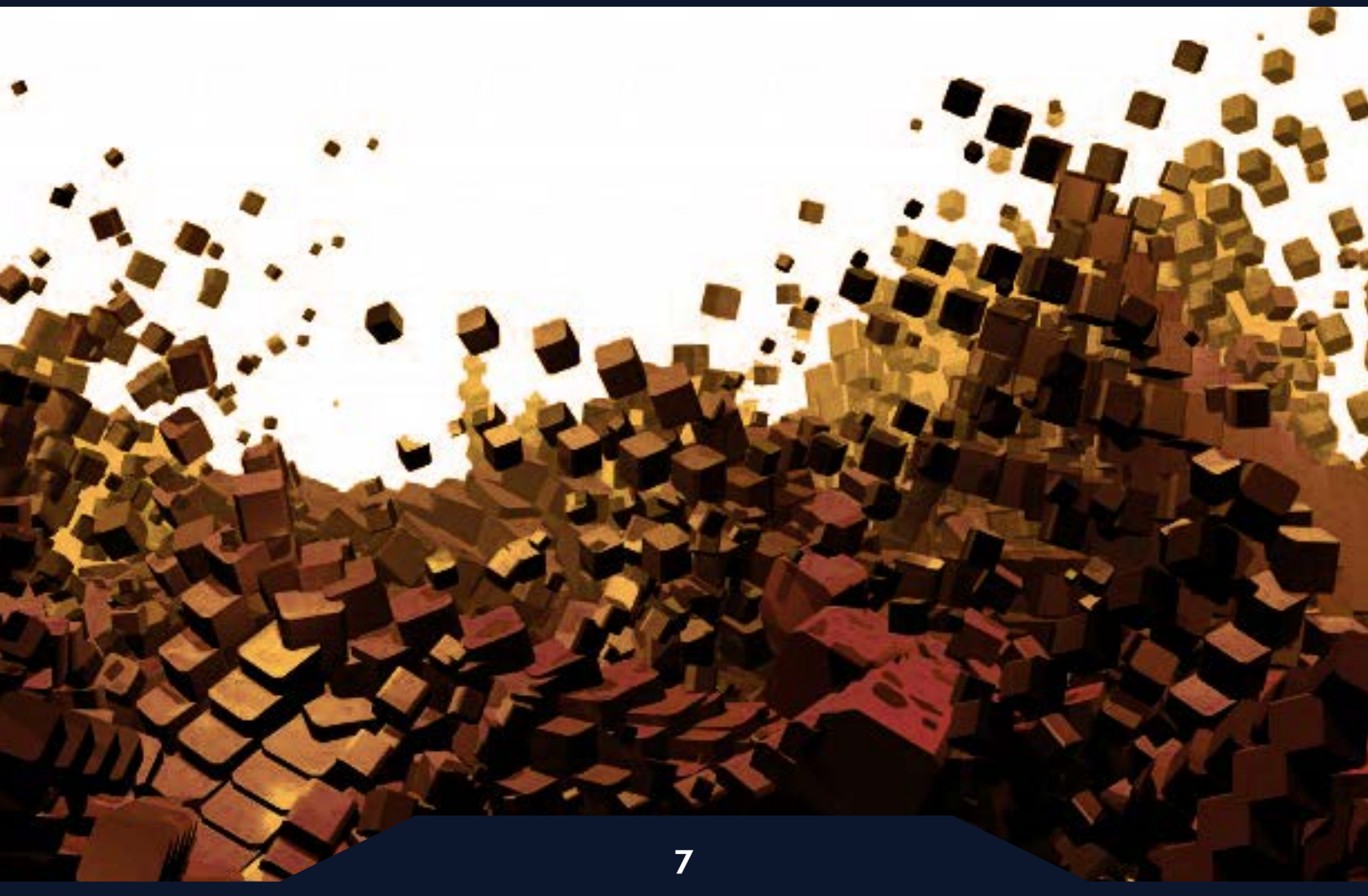
Diversity

Marymount is classified as one of the most diverse universities in the south, as designated by U.S News and World Report. This is reflected in our master's in cybersecurity program. Of particular significance, is our 50 percent female participation in the program, much higher than the workplace average of 11 percent. Also, Marymount is classified as Veteran friendly and supports the Yellow Ribbon program.

Job Expectations

Arlington, VA is a great location, and cybersecurity positions come up on a daily basis. The University posts relevant positions to its Cyber Center Canvas site, and this is a great resource whether looking for an internship or a full-time job. Also, alums and working students actively recruit from students in the program at Marymount.

Tackling the Application: Preparing to Apply to a Program



Tackling the Application: Preparing to Apply to a Program

Prerequisites

Find out what prerequisites a program prefers. Many programs want you to have a bachelor's degree or certification in a related discipline, such as computer science, software development or information technology. Some even specify a GPA requirement of a 3.0 or above for all or the last half of undergraduate studies.

If you don't have a computer-related bachelor's, some programs will look for high grades in courses with related skills such as statistics or calculus. Some programs consider relevant professional experience.

Even if you don't have relevant experience or undergraduate coursework, you can still apply to a cybersecurity master's program. Just be prepared for the program to require you to take certain courses first. You may want to take some anyway, regardless of whether or not it is required. It can position you to succeed once you get into a program.

Work Experience

Because cybersecurity is highly technical and skills-based, work experience is heavily favored. Some programs even require a minimum level of computer-related work experience. Make the most of your relevant work experience by highlighting it on your resume and in your application.

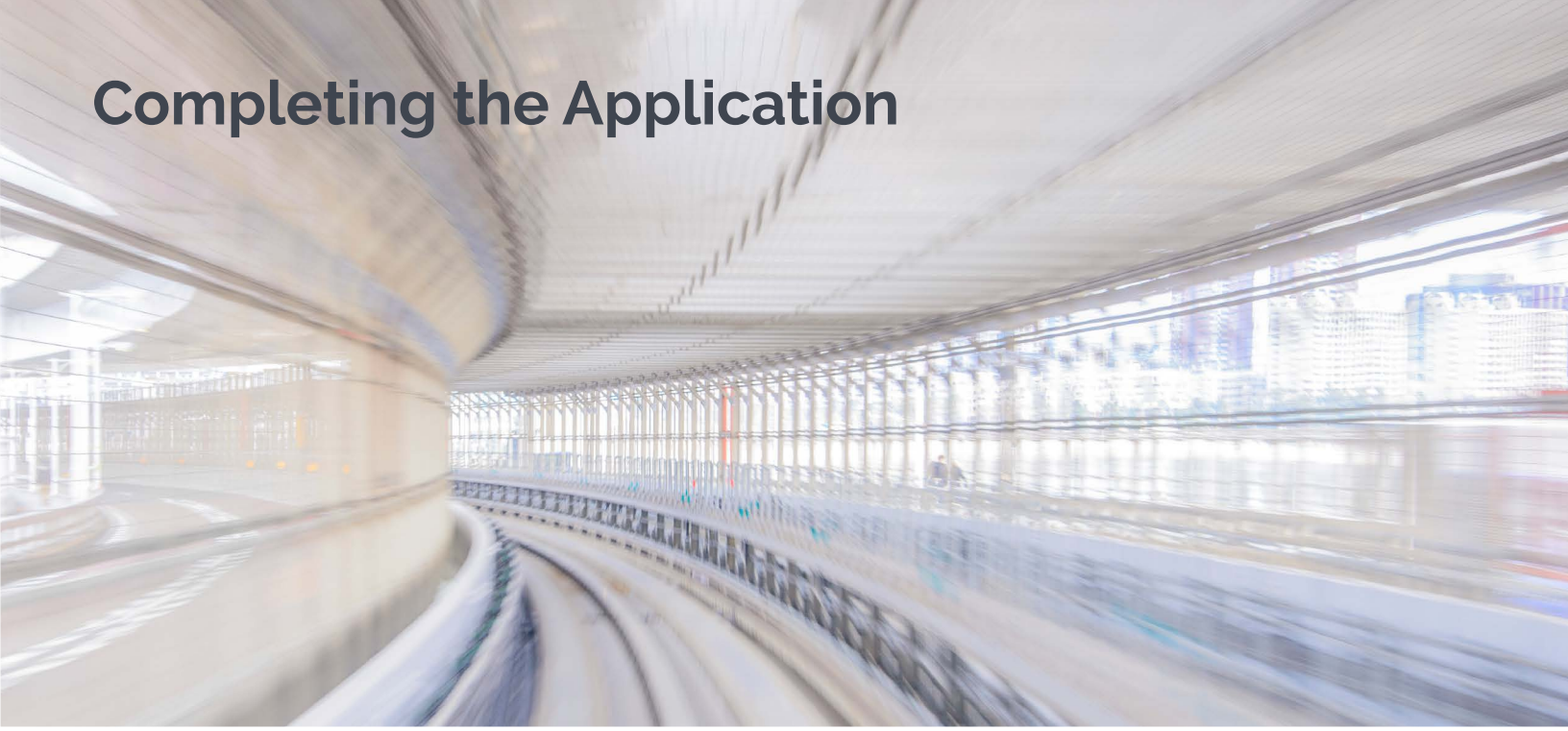
Exams

Check to see if you need to take an exam for admission. Some programs require you to take the GRE or GMAT, but many do not. International students may also be required to pass the TOEFL (or equivalent) to demonstrate a high level of English language proficiency.

Find out what the program you are interested in requires. If you do need to take an exam, allow yourself time to prepare for it. Most students take three to six months to prepare for the GMAT or GRE, and some may take an online class or hire a tutor. Taking practice tests is a good way to gauge your progress and to focus your preparation efforts.

Did you know? 44% of online adults have experienced cyber crime in the last year

Completing the Application

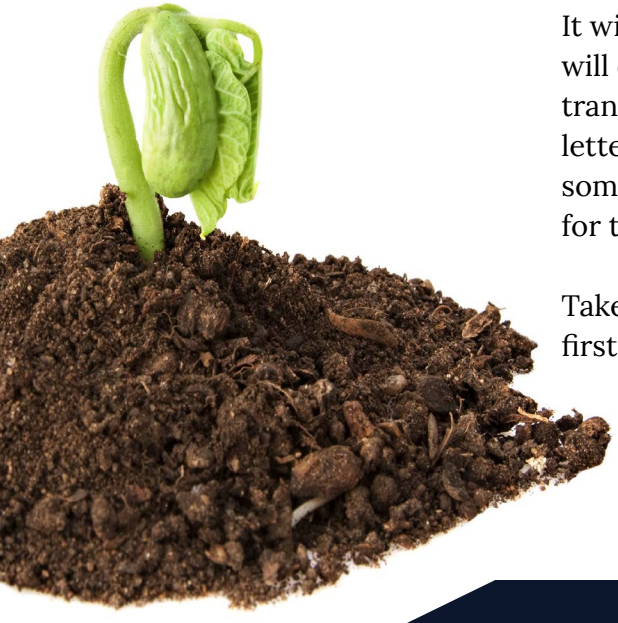


Do Your Research and Plan Ahead

Each program has its own application requirements and application deadlines. Research the requirements of all the programs you want to apply to. Make a plan for taking any exams or courses, obtaining all the necessary pieces of information, and completing your applications.

For example, you will probably need an official copy of each of your higher education transcripts for each application. But plan ahead and order a few more copies just in case you discover you want to apply to another program.

Give Yourself Time



It will take time to research master's programs, determine what credits will count toward a program's requirements, obtain copies of your transcript, prepare for the GRE or GMAT if required, solicit and collect letters of recommendation, and fill out applications. If you need to take some extra courses before even applying to a program, you'll need time for that, too.

Take the time to do them all well. Your application will be a program's first impression of you, and you want it to be a good one.

Completing the Application

Statements of Purpose

Many applications will ask for a statement of purpose, your motivation for wanting to pursue a master's degree in cybersecurity. Consider what kind of statement each program requires, and prepare a statement of purpose that can be used, with only slight modifications, for each application.

Letters of Recommendation

You'll also want to plan ahead for soliciting letters of recommendation. Choose carefully among your current (or former) professors and co-workers to find the people who are in the best position to highlight your strengths. You can be strategic by asking people who are graduates of the programs you are applying to or who are experienced in the field.

However, make sure the recommender actually knows you. While it may be nice to submit a recommendation from an impressive name, it is more important that your recommender can genuinely speak to your strengths.

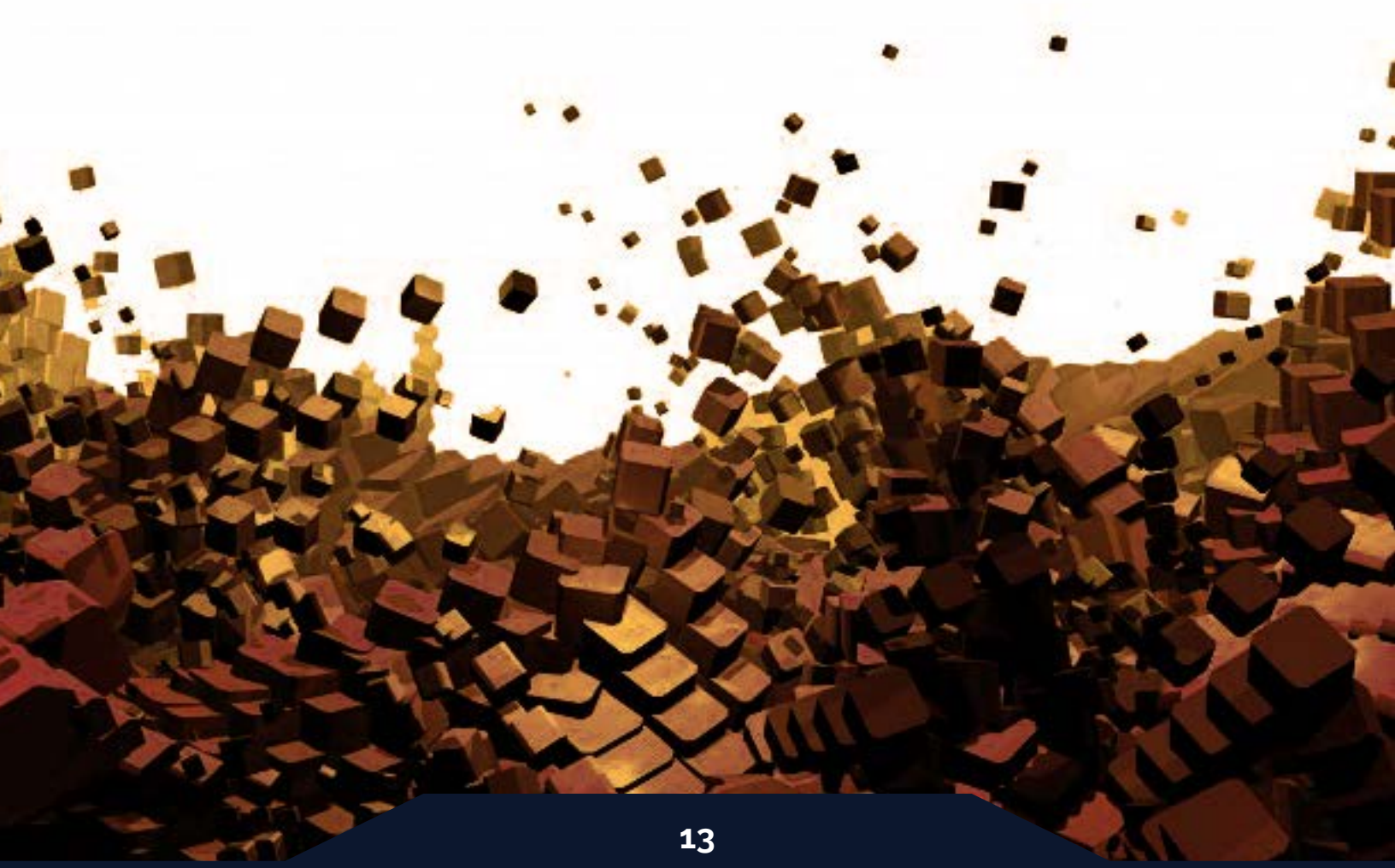
Just as importantly, make it easy for your recommenders to help you. Give them at least three to four weeks to prepare and mail their letter of recommendation. Provide them with a packet that reminds them of the deadline and how many copies you need, include pre-addressed, stamped envelopes, and give them information about the programs that you think will help them prepare a thoughtful letter. If your recommender is a former professor or co-worker, you may want to include a reminder of some of your traits and accomplishments during your time with them.

Many institutions now require the recommendations to be submitted through an online form, however, most allow a written letter of recommendation to be submitted with the form.

Did you know?

90% **of private sector business have been hit by a security breach in the past year**

Job Opportunities



Job Opportunities

Common Job Titles

Note: There are no standard job titles in cybersecurity: Some companies use terms such as cybersecurity, others use information security, or information assurance. The Federal government still refers to them as IT Specialists.

Some job titles might be for those with a master's degree in cybersecurity:

- Cybersecurity Analyst/Engineer
- Cybersecurity Architect
- Cryptographer/Cryptologist/ Cryptanalyst
- Chief Information Security Officer
- (CISO)
- Cybersecurity Consultant
- Information Assurance Engineer

Top Employers

- Accenture
- Amazon Web Services
- Booz Allen Hamilton
- Deloitte
- General Dynamics
- IBM
- Northrop Grumman
- Science Applications International Corporation

As digital technology becomes ever more ubiquitous, cyber attacks have grown with it, and consequently, the need for cybersecurity professionals has increased dramatically. Cybersecurity is quickly becoming the most sought-after career in technology. As cyber threats continue to grow, the need for experienced and knowledgeable cybersecurity professionals remain in-demand.

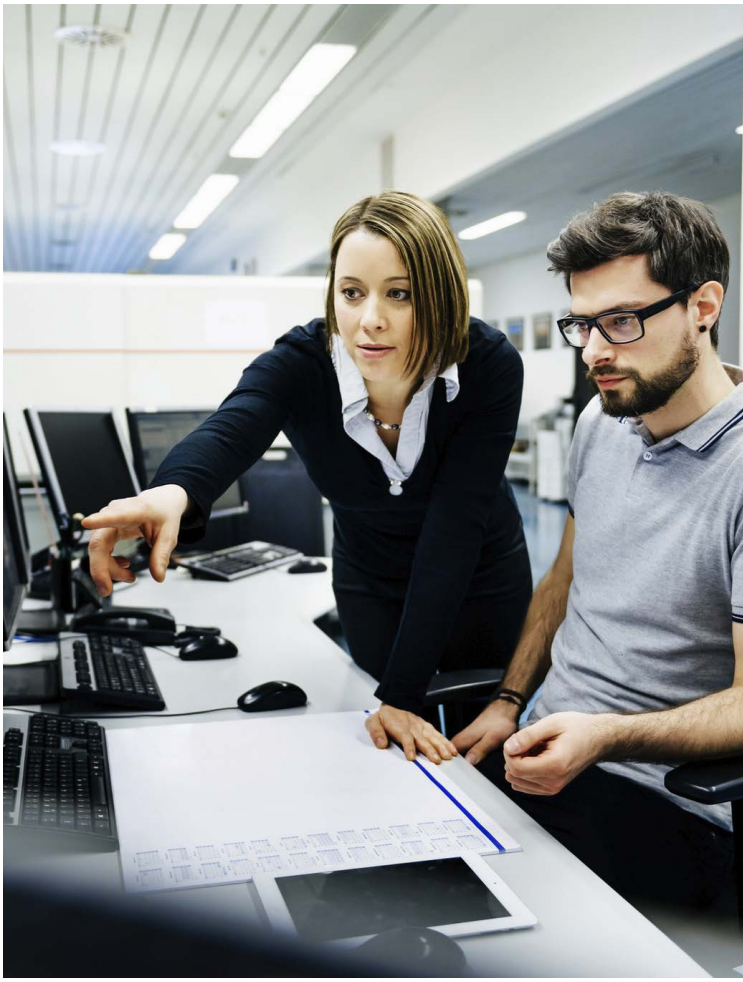
Currently, there are roughly half a million cybersecurity-related job openings in the United States with a projected need for 1.8 million additional cybersecurity professionals to fill the workforce gap by 2022. Cybersecurity jobs offer salaries three times the national average and getting a master's degree increases your chances of landing a highly paid and rewarding position.

Did you know?

The Senate Security Operations Center gets 13.9 million cyber attacks per day

Job Opportunities

In a survey recently conducted by the SANS Institute, 49 percent of respondents — cybersecurity professionals — reportedly make $100,000 or more. Further breaking down the data, they report that the highest figures are "mostly attributed to those with management roles, while the largest single group (23 percent) selected the $80,000–$99,999 range, representing those with administrator or engineering roles."



Where does a master's degree fit into all of this?

The SANS Institute also found that while experience in the field is a sure path to increased salary, professionals with master's degrees get higher salaries sooner.

Consider the following graph:

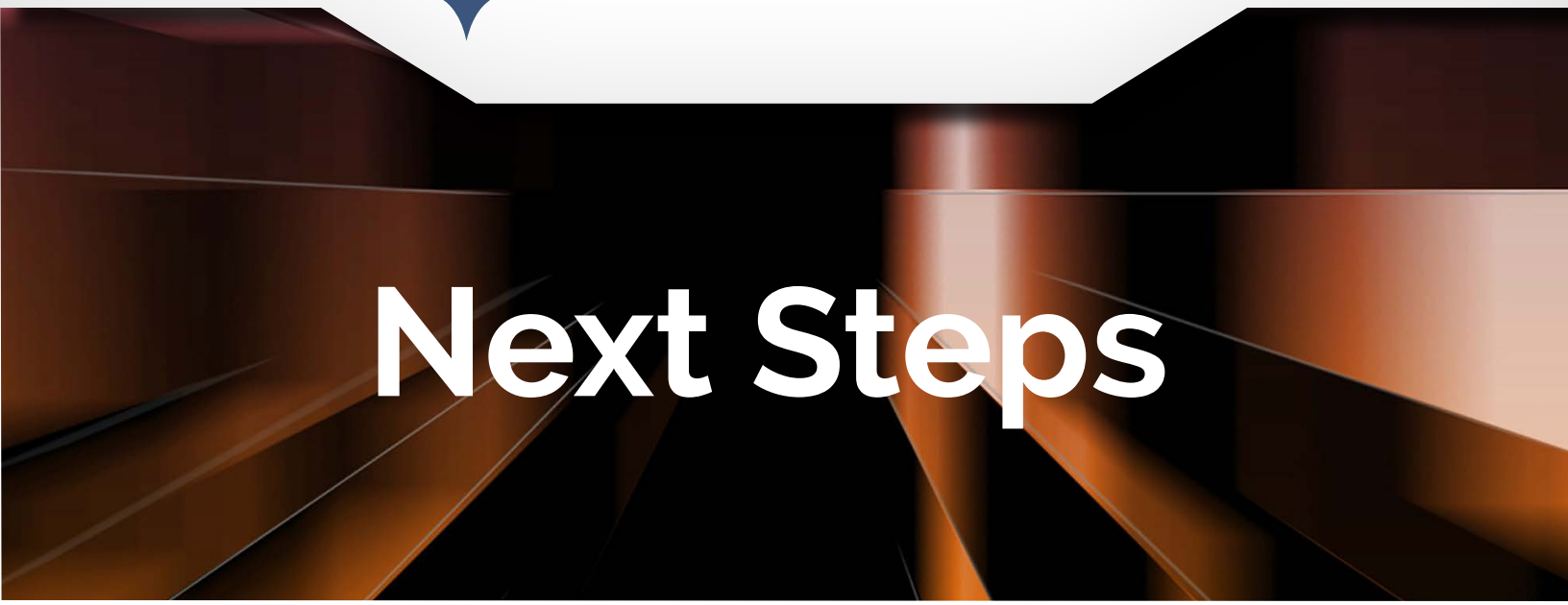
Income by Education Level and Years of Experience

Education	0-3 YRS	4-6 YRS	7-10 YRS	11-15 YRS	16-20 YRS	+20 YRS	Overall
Bachelor's Degree	$71,564	$84,619	$100,862	$115,782	$123,561	$127,733	$98,510
Master's Degree or MBA	$82,906	$97,109	$109,319	$120,964	$132,816	$125,464	$109,705

* Source: The SANS Institute

The difference of these salaries over time widens the gap even further. While graduate school is an investment, it pays for itself over and over again with a high salary earned earlier in your career.

MARYMOUNT UNIVERSITY



Next Steps

The Marymount Admissions team hopes this enlightening and informative guide will provide you with the necessary resources to reference and the opportunities to consider as you prepare for the next step in your academic career.

Have a question about our M.S. in Cybersecurity? We invite you to request more information today!

Request More Information

If you're looking for more stories related to trends, news, and advice related to graduate school, subscribe to our weekly graduate education blog — The Next Degree!

Subscribe Today

@marymountu

Facebook.com/
Marymount.University