Your Career in Cybersecurity

What's Ahead for Graduates with a Master's Degree in Cybersecurity?

SAINT LEO UNIVERSITY
125
YEARS
·Est. 1889·

A Saint Leo University E-Book for Adult Online Learners

Purpose of this E-book

The list of companies that have fallen victim to data breaches involving customers' credit and debit accounts grows every day.

Private businesses are not the lone victims of cybercrime. Governments, health care, finance, law enforcement and academia all need information security professionals who can protect their organizations' data assets. Even the president of the United States has said that America's economic prosperity in the 21st century depends on cybersecurity.

BUT RIGHT NOW, THERE'S A CRITICAL SHORTAGE OF QUALIFIED CYBERSECURITY PROFESSIONALS.

In other words, the field is teeming with career opportunity.

That's why we created this e-book – to give you an overview of the growing field of cybersecurity and the opportunities that may be available to you with an advanced degree. It's a quick read filled with valuable information about industry trends, career paths and certifications to advance your career.

We hope you find it helpful as you plan your next move in the cybersecurity field.

> **"The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront.**
>
> **The national and economic security of the United States depends on the reliable functioning of the nation's critical infrastructure in the face of such threats."**
>
> *— Presidential Executive Order, 2013*
> *Improving Critical Infrastructure Cybersecurity*

НАСОС ЭЖЕКТОРНОГО КОНТУРА (К54)
БАК ЭЖЕКТОРНОГО КОНТУРА (К55)
В28
БАК ДЕАЭРИРОВАННОЙ ПОДПИТОЧНОЙ ВОДЫ (К56)
10 13 14 15 16 17
YA10
YA11
5°C
FQI
TI G3
TI G4

Contents

TRENDS

CAREER PATHS

ADVANCING YOUR CAREER

Share this e-book:

online.saintleo.edu

Trends

CYBERCRIME: BIG BUSINESS

The cybersecurity field is exploding with opportunity. It's no wonder; cybercrime is big business, and no one is immune.

A 2014 report by security software maker McAfee and the Center for Strategic and International Studies (CSIS) puts the global cost of cybercrime at more than $400 billion per year. According to a 2014 Verizon study, 97 percent of small to mid-size businesses have been hacked – and most don't even know it.

That's just the tip of the iceberg. Consumers, governments and the private sector are increasingly falling victim to cybercrime.

Consider these statistics:

- Between 2013 and 2014, 40 million people in the United States had their personal information stolen, according to the McAfee/CSIS study, along with 54 million people in Turkey, 20 million in Korea, 16 million in Germany and more than 20 million in China.
- In the 12 months between 2012 and 2013, data breaches increased by 62 percent, according to security services provider Symantec.

The need for information security specialists who can predict, prevent and react to cyber threats swiftly and precisely becomes more urgent every day.

Trends

ACUTE SHORTAGE OF PROFESSIONALS

While the demand for cybersecurity practitioners is growing exponentially, there is an acute shortage of professionals trained to protect vital computer networks and electronic infrastructures from attacks.

- According to Burning Glass Technologies, demand for cybersecurity skills has increased more than four times faster than for any other IT jobs over the past five years and more than 12 times faster than for all other non-IT jobs.

- In 2013, cybersecurity job postings took 24 percent longer to fill than all IT job postings and 36 percent longer than all job postings, according to Burning Glass.
- Twenty-five percent of organizations describe a shortage of employees with in-demand skills, Symantec reports, and 83 percent of companies say they lack the skills and resources to protect their IT interests.

BOTTOM LINE, THERE'S NEVER BEEN A BETTER TIME TO CONSIDER A FUTURE IN CYBERSECURITY.

GO TO CONTENTS

Trends

NATIONWIDE DEMAND

The shortage of cybersecurity professionals spans nearly every region and every industry in the nation. According to the Burning Glass report, the Washington metropolitan area had more than 23,000 postings for cybersecurity positions in 2013 – surpassing any other region in the nation. But demand wasn't limited to the nation's capital, the report says.

- New York City, with more than 15,000 postings, had the second-highest number of postings in 2013.
- The San Francisco-San Jose metro area had more than 12,000 postings.
- Atlanta reported the highest percentage growth of cybersecurity postings since 2007, with 213 percent growth.
- By state, demand for cybersecurity professionals was greatest in California, followed by Virginia, Texas, New York, Illinois, Maryland, Florida and Massachusetts.

GO TO CONTENTS

Trends

A MULTI-INDUSTRY CONCERN

The demand for cybersecurity professionals is a concern for every sector and segment of the nation's economy, with the professional services sector leading the pack. According to the Burning Glass report, the leading industries for cybersecurity professionals are:

INDUSTRY	# OF JOB POSTINGS IN 2013
Professional Services	80,446
Manufacturing & Defense	28,331
Finance & Insurance	24,145
Information	15,820
Health Care	12,257

While professional services leads in number of jobs posted, the greatest growth industries for cybersecurity professionals are finance and insurance, followed by health care.

GO TO CONTENTS

Trends

WHAT'S BEHIND THE GROWTH?

So why is the field of cybersecurity growing by leaps and bounds?

The answer is simple: increasing vulnerability at every level. Consider the number of devices at our disposal – laptops, desktops, iPhones, wearable computers, gaming systems and more. The sheer explosion in points of entry, not to mention cloud computing, opens whole new areas of vulnerability.

> **"Cybercriminals are getting better at circumventing firewalls and antivirus programs. More of them are resorting to ransomware, which encrypts computer data and holds it hostage until a fee is paid. Some hackers plant virus-loaded ads on legitimate websites, enabling them to remotely wipe a hard drive clean or cause it to overheat..."**
>
> **— *New York Times*, 2014**

And that's just one piece of it. There are additional reasons the field is hot:

- **Increasing size and scale:** The reach of cybercrime is growing by the hour, and is now at a point where consumers and regulators are demanding action. While the McAfee/CSIS study conservatively puts the global cost of cybercrime at more than $400 million, experts say it could be as high as $575 million.
- **No one is immune:** Consumers, businesses and agencies are increasingly getting hacked. The Target breach alone affected tens of millions of consumers; a 2013 breach of Adobe customers' identity and encrypted information affected more than 152 million people. And cybercrime is hardly limited to hacking.
- **The competitive market is rewarding innovation:** Dominant information security companies and antivirus programs alone are no match for growing cyberthreats, according to Gartner analysts. New and innovative solutions are needed, raising the appeal of new entrants to the information security market.
- **A changing game of cat and mouse:** The field of cybercrime is constantly changing, and there's no shortage of cybercriminals working feverishly to crack the latest code. Cybersecurity professionals are needed to develop new models.

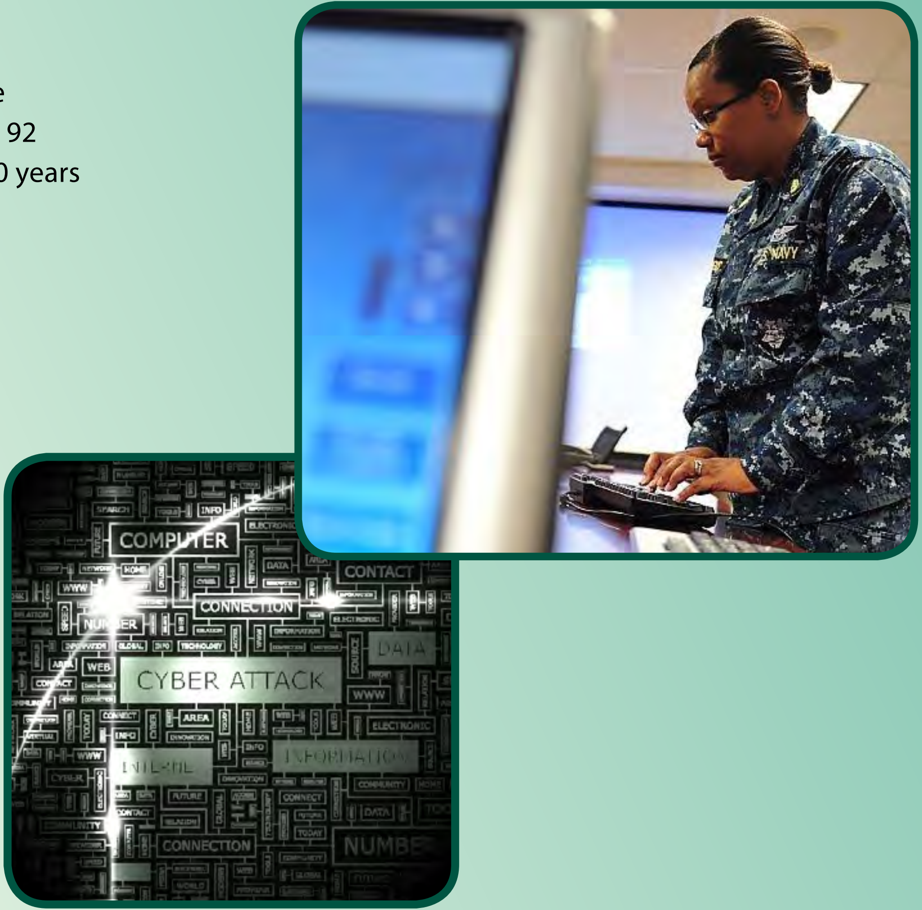
GO TO CONTENTS

Trends

HOW'D THEY DO THAT?

According to the 2014 Verizon study, in spite of the seemingly limitless threats to information security, 92 percent of 100,000 incidents analyzed in the last 10 years can be described by nine basic patterns:

- Point of sale intrusion
- Cyberespionage
- Physical theft and loss
- Payment card skimmers
- Web app attacks
- Crimeware
- Insider misuse
- Denial of Service (DOS) attacks
- Miscellaneous errors



GO TO CONTENTS

Trends

LEGAL HACKING

More and more, business and government entities are turning to ethical hackers to assess vulnerabilities in computer systems. These legal "bad guys" use their expert computer skills to penetrate enterprise networks and infrastructure, much like traditional hackers, but not for mischief or personal gain. Their goal is focused – to protect an organization's computer systems by thinking and working from a hacker's point of view.

A 2012 article in *PCWorld* magazine calls the job market for ethical hackers "extremely good." With professional IT experience a requirement for the job, the publications says ethical hackers can earn between $50,000 and $100,000 in their first year, and $120,000 or more per year with several years of professional experience.

GO TO CONTENTS

Career Paths

THE TIME IS NOW

The time is now to get your start in the exciting field of cybersecurity. At the national level, the Bureau of Labor Statistics (BLS) projects significant employment growth for all cybersecurity occupations, with particularly strong 10-year percentage growth for:

- Database administrators – 30.6 percent
- Network and computer systems administrators – 27.8 percent

According to the Bureau of Labor Statistics , computer systems analysts will comprise the largest number of jobs between 2010 and 2020, adding 222,500 new jobs.

Career Paths

REWARDING CAREER OPTIONS

Still wondering what to expect from a career in cybersecurity? Let's take a look at five job titles from the Bureau of Labor Statistics.

- **Computer and Information Systems Manager (often called IT Manager)**

  What you might do: Plan, direct or coordinate computer-related activities in areas such as electronic data processing, information systems, systems analysis and computer programming. Help determine an organization's information technology goals and implement systems to meet those goals.

  What you might earn: The BLS reports a median annual salary of $123,950 for this job.

- **Computer Systems Analyst**

  What you might do: Analyze an organization's computer systems, requirements, procedures and problems to automate or improve existing systems. Serve as an interface between the business and its information technology needs and limitations.

  What you might earn: The BLS reports a median annual salary of $79,680 for this job.

- **Information Security Analyst**

  What you might do: Plan, design and carry out various measures to protect an organization's computer networks and systems from attacks both internally and externally. As the number of threats and cyberattacks continues to increase, so does the size and scope of the security analyst's responsibilities.

  What you might earn: The BLS reports a median annual salary of $86,170 for this job.

- **Database Administrator**

  What you might do: Use specialized software to store and organize data, such as financial information, customer shipping records, student grades, voter data and more. Ensure that data is available to many different users in an organization – and not available to unauthorized users.

  What you might earn: The BLS reports a median annual salary of $77,080 for this job.

- **Network and Computer Systems Administrator**

  What you might do: Oversee and ensure the day-to-day operation of an organization's network LANs, WANs and intranets, working directly with the organization's physical computer networks.

  What you might earn: The BLS reports a median annual salary of $72,560 for this job.

GO TO CONTENTS

Career Paths

AT WORK EVERYWHERE

Cybersecurity professionals are at work everywhere – in the public and private sectors, part time and full time, in virtually every industry in every country around the world.

According to Symantec's 2013 study, government agencies face the greatest shortage of IT security professionals. Thirty-six percent of government agencies reported a "severe lack" of security professionals, followed by manufacturing, financial services and retail enterprises.

Interested in a career abroad? You're in luck. According to the McAfee/CSIS report, the countries with the highest levels of cybercrime relative to gross domestic product are Germany and the Netherlands, with 1.6 and 1.5 percent, respectively, followed by Norway, the United States, China, Singapore, and the European Union.

Country	% of GDP
Germany	1.6
Netherlands	1.5
Norway	.64
United States	.64
China	.63
Singapore	.41
European Union	.41

Did you know?

According to a 2013 Global Information Security Workforce Study, women represent only 11 percent of the information security workforce worldwide.

Career Paths

OPPORTUNITIES ABOUND

At every level, in every sector, in just about every region of the world, cybercrime is a growing threat with serious implications for trade, competitiveness, innovation and global economic growth. Yet finding workers who have the necessary skills to fill cybersecurity jobs is a growing challenge.

According to the Burning Glass report:

- 84 percent of cybersecurity job postings require at least a bachelor's degree
- 67 percent require at least four years' experience.

PROFESSIONALS WITH EXPERIENCE AND AN ADVANCED DEGREE HAVE THE GREATEST CAREER ADVANTAGE.

What You Could Be

The sky's the limit for skilled cybersecurity professionals. More and more, these experts are filling c-level posts, including chief information officer (CIO) and increasingly, chief information security officer (CISO). According to salary.com research, the median annual salary for a chief information technology officer in the United States in 2014 is $244,244.

For entrepreneurial types, the field for cybersecurity consultants is wide open. Cybersecurity consultants are among the most sought-after professionals in the tech sector. A 2013 report from industry research firm IBISWorld says the cybersecurity industry is expected to expand by 7.7 percent annually, reaching 285.9 billion in revenue by 2018.

Specialists who work with specific systems, including network engineers, network security engineers and systems security engineers are also in demand, as are risk management specialists, responsible for monitoring compliance and assessing a company's risk for cyberthreats.

GO TO CONTENTS

Advancing Your Career

EARNING CERTIFICATIONS

Cybersecurity jobs require both education and experience, but many of the best jobs require something more. According to Burning Glass, 51 percent of all cybersecurity positions require at least one of the certifications below:

CERTIFICATION		% OF POSTINGS
CISSP	Certified Information System Security Professional	24
CISA	Certified Information Systems Auditor	16
Security+	Certified Information Security Manager	8
CISM	Certified Information Security Manager	7
GIAC	Security Essentials	3
CIPP	Certified Information Privacy Professional	2
SSCP	Systems Security Certified Practitioner	2
GIAC GCIH	Certified Incident Handler	2

While this list includes some of the most commonly requested certifications, it does not include all certifications available to cybersecurity professionals today. A number of entry-level certifications offered through **CompTia** (certifications with a + in the title such as A+, Network+ and Security+) and topic-specific certifications, such as Certified Ethical Hacker (CEH), are allowing cybersecurity professionals to hone in on specific cybersecurity skills.

Advancing Your Career

PURSUING A GRADUATE DEGREE

For information technology, computer science and cyberoperations professionals, an advanced degree in cybersecurity can be an important step along the path to a successful career in the growing field of cybersecurity.

Here are some reasons why you might want to consider a graduate degree program:

1. **You have been working in the information technology field, but your bachelor's degree is in an unrelated discipline.**

   If this describes you, it may be time to consider pursuing a degree related to your field. Obtaining the academic credential specifically targeted at your career path can go a long way toward advancing you to the next level.

2. **You have a bachelor's degree in computer science, management information systems, computer information systems or a related area.**

   While your undergraduate degree provides a solid foundation, earning a graduate degree in cybersecurity is a good way to gain advanced, specialized knowledge to prepare you for this highly technical field.

3. **You want to advance your IT or cybersecurity career.**

   If you're an experienced professional, earning an advanced degree will enhance your skills and provide you with the deeper knowledge that will enable you to step up to the next level in your career or to pursue consulting work.

4. **You have earned leading professional certifications in the cybersecurity field.**

   Even if you have any number of entry-level, advanced or specialized professional certifications under your belt, if your undergraduate degree is in an unrelated discipline, earning a graduate academic degree will give you the academic credential and recognition you need.

5. **You have a deep understanding of the design, administration and management of operating systems and networks.**

   If you already have strong foundational knowledge and skills, you are well prepared for a deep dive into the technical aspects of information security that a graduate degree program in cybersecurity offers. It's a natural next step toward a valuable credential.

GO TO CONTENTS

Advancing Your Career

ONLINE GRADUATE PROGRAMS AT SAINT LEO

Since 1998, Saint Leo University has been a leading provider of online education to working adults and is a major global provider of education to the military. The university provides innovative, rigorous and engaging **graduate degree programs** that address current and emerging issues in fields ranging from sport business to critical incident management to educational leadership.

Saint Leo's Master of Science in Cybersecurity

Saint Leo University's innovative **Master of Science in Cybersecurity** educates students in the technical aspects of cybersecurity systems. The program provides graduates with the knowledge, critical analysis and application skills needed to assume leadership positions in the fields of information assurance and computer security.

Graduates of the 36-credit hour degree program are prepared to:

- Protect the information systems of different types of organizations
- Support the nation's information infrastructure
- Conduct advance research in information security and assurance
- Work in federal, state and local governments, as well as the private sector and academia

The program is aligned with the core curriculum for graduate information assurance degrees set forth by the National Security Agency (NSA) and with the knowledge units covered in many industry-recognized professional certifications in information security, such as Security+, CISSP, SSCP, CSSLP and CISM.

For more information about Saint Leo's Cybersecurity program, visit us online at **online.saintleo.edu.**

You can also call to speak with one of our graduate enrollment counselors at 800.707.8846.

About Saint Leo University

In 1889, **Saint Leo University** was founded by the Order of Saint Benedict and chartered by the State of Florida. Since then it has remained one of the nation's premier Catholic, coeducational liberal arts universities, serving people of all faiths and backgrounds.

Saint Leo's scenic, 150-acre University Campus is located in the heart of Florida, just 30 miles north of Tampa and 90 miles west of Orlando. The university enrolls more than 16,000 students across our traditional campus, online degree programs, and more than 40 teaching locations, including 14 on military bases in six states.

Core Values

Since Saint Leo's founding, the university's aspiration has been to provide students with one-on-one attention, flexible learning opportunities, and a solid foundation for personal fulfillment and career advancement. To assist students in becoming successful scholars and citizens, Saint Leo emphasizes these core values:

- Excellence
- Community
- Respect
- Personal Development
- Responsible Stewardship
- Integrity

GO TO CONTENTS

Sources

Chief Information Technology Officer Salaries, salary.com 2014, **http://www1.salary.com/Chief-Information-Technology-Officer-Salary.html**

Cool Vendors, Gartner 2014, **http://www.gartner.com/technology/research/cool-vendors/**

Data Breach Investigations Report, Verizon 2014, **http://www.verizonenterprise.com/DBIR/2014/**

Executive Order – Improving Critical Infrastructure Cybersecurity, **http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity**

(ISC)2 Global Information Security Workforce Study, Frost & Sullivan 2013, **https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/2013-ISC2-Global-Information-Security-Workforce-Study.pdf**

Hackers Find New Ways to Breach Computer Security, New York Times 2014, **http://www.nytimes.com/2014/06/22/sunday-review/hackers-find-new-ways-to-breach-computer-security.html**

How to Become an Ethical Hacker, PCWorld 2012, **http://www.pcworld.com/article/250045/how_to_become_an_ethical_hacker.html**

Internet Security Threat Report, Symantec 2014, **http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf**

Job Market Intelligence: Report on the Growth of Cybersecurity Jobs, Burning Glass Technologies 2014, **http://www.burning-glass.com/media/4187/Burning%20Glass%20Report%20on%20Cybersecurity%20Jobs.pdf**

Net Losses: Estimating the Global Cost of Cybercrime, Center for Strategic and International Studies 2014, **http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf**

Occupational Outlook Handbook, 2014-15 Edition, Bureau of Labor Statistics, U.S. Department of Labor, **http://www.bls.gov**

Security Breach: 10 Industries Impacted, IBISWorld 2013, **http://www.ibisworld.com/media/2013/04/15/security-breach-10-industries-impacted/**

GO TO CONTENTS

It's your time to **shine**.

Saint Leo Honors Your Commitment

We celebrate your decision to finish what you started with a degree from Saint Leo University—a trusted leader in adult and online education.

SAINT LEO
UNIVERSITY®

Undergraduate
888.875.8265

Graduate
800.707.8846

Learn More About Saint Leo University's Online Degree Programs

REQUEST INFORMATION

Share this e-book:

A Saint Leo University E-Book for Adult Online Learners