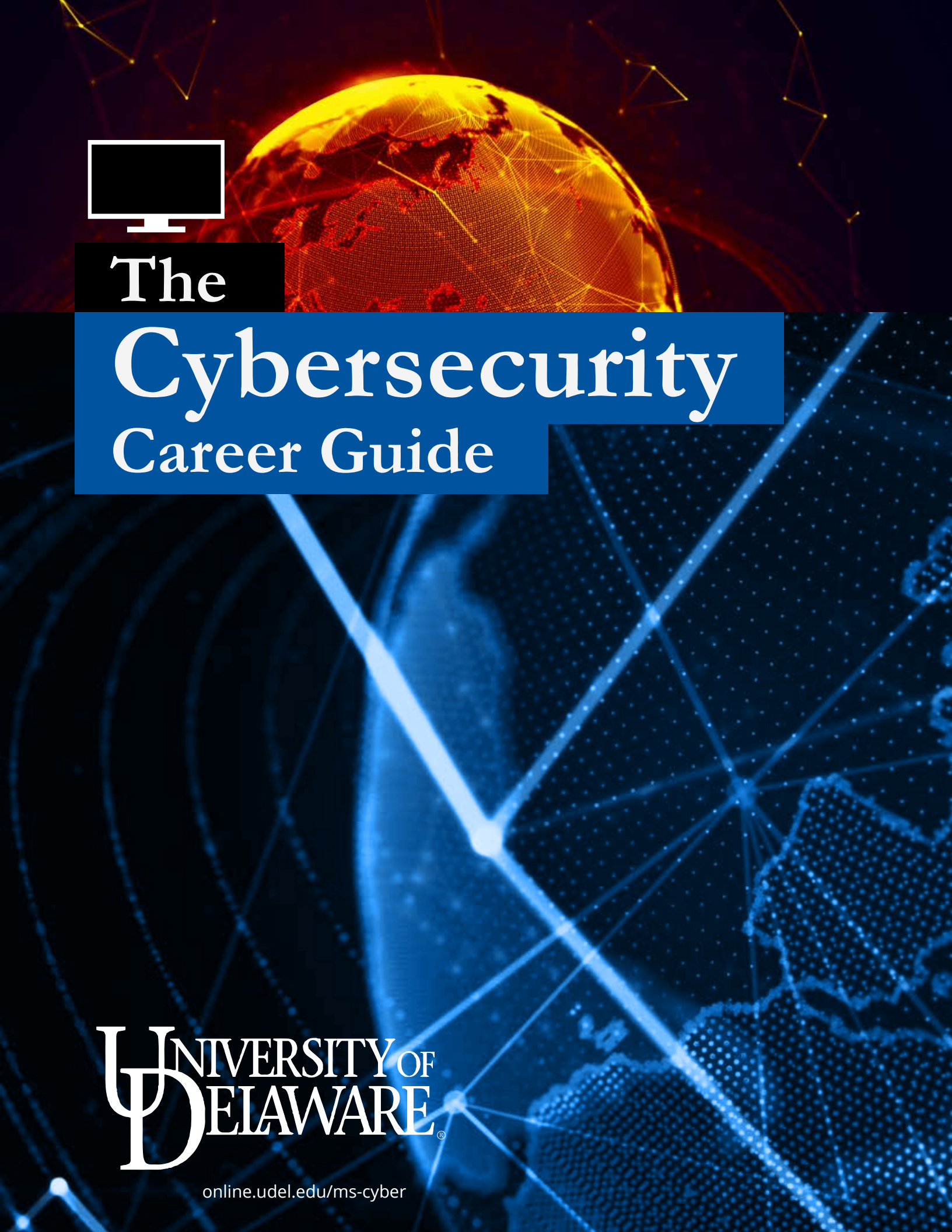


The Cybersecurity Career Guide

UNIVERSITY OF DELAWARE

online.udel.edu/ms-cyber

At the beginning of 2016, Forbes magazine reported that more than 200,000 cybersecurity jobs in the United States were unfilled.

Cloud computing, big data, and 'the internet of things' have become ubiquitous. Information has become the most powerful global asset – yet it remains one of the most vulnerable. Hackers have breached design files of critical U.S. weapons systems, stolen 170 million ATM and credit card numbers, and disabled power systems that provide electricity to hundreds of thousands of people. President Obama said the growing number of attacks on our cyber networks has become *"one of the most serious economic and national security threats our nation faces."*

From online banking to online medical records, from secure credit card data to secure military communications, cybersecurity is the world's new sentinel.

This new global paradigm, however, can translate into opportunity – career opportunity. In fact, the United States Bureau of Labor Statistics predicts 18% growth in the industry between 2014-2024. Cisco estimated a million cybersecurity job openings globally in 2016. The CEO of the security-software company Symantec expects job openings to grow to 6 million globally in the next three years. Careers in cybersecurity are also lucrative; Burning Glass Technologies has stated that professionals in cybersecurity earn almost 9% more than their counterparts in IT, and the Bureau of Labor Statistics says that 2015 median pay was more than $43 an hour for cybersecurity engineers – totaling more than $90,000 a year.

Here's a guide to some of the careers available in the cybersecurity world today:

Cybersecurity Careers by Industry

Utility Companies: Electricity, Water, Natural gas, and Infrastructure

It's hard to imagine anything as basic and essential to our ways of life as electricity, water and natural gas. They are necessities, and they affect every home in the nation. *"The worst-case scenario is a critical infrastructure attack, and these organizations are ill prepared to deal with it,"* says Dr. Larry Ponemon, founder of the Ponemon Institute. Oil and gas pipelines crisscross the nation, many above ground. Hackers could interrupt service, hold an electrical grid hostage, or infiltrate the water systems.

"Cybercriminals are constantly on the lookout for new targets they can exploit for information and financial gain," says the IT security company Trend Micro. *"Recently, however, research shows these virtual criminals are increasingly putting the technological systems of a new sector in their crosshairs: utility providers."*

Job responsibilities:

- Analyzing risk of cyberattack
- Designing and implementing cybersecurity systems as they relate to the electric grid and gas, oil and water delivery
- Focusing on proactive cyber-threat detection and response
- Implementing security best practices
- Understanding global utility threat environment

- Problem-solving and analysis
- Working on multiple platforms
- Leading meetings and project teams

Prefered job requirements:
Perhaps the most common requirement for a successful career in the utility sector is the Certified Information Systems Security Professional (CISSP) credentials. This certification requires a candidate to have:

- 5 years' cumulative full-time paid work experience, or a four-year college degree
- 4 years' cumulative full-time paid work experience, or pass the CISSP exam
- Accumulate the required experience in the 6 years following

Other possible requirements or preferred certifications can be Certified Ethical Hacker (CEH), SANS GIAC Certified Industrial Cyber Security Professional (GICSP) or SANS GIAC Certified Penetration Tester (GPEN).

Job examples:

- Principal Cybersecurity Architect/Engineer: Pacific Gas & Electric Company, San Francisco
- Lead Cyber Security Systems Engineer: The Parsons Corporation in Centreville, Virginia
- Threat & Forensics Engineers: The Bergalia Companies, Houston
- Critical Infrastructure Security Analysts: Idaho's Natural Laboratory's National & Homeland Security Directorate

Career outlook:
National salaries for professionals in this sector range from $80,000 – $85,000. The infrastructure of the nation's utilities is aging while the threats increase. In 2014, NSA Director Admiral Michael Rogers said several foreign governments had already hacked into U.S. energy, water and fuel distribution systems, potentially damaging essential services. "This is not theoretical," Rogers said. "This is something real that is impacting our nation and those of our allies and friends every day."

Telecommunications: Phones, Cable providers, and Wi-Fi

A case study by the professional services company Deloitte points out the irony of the vulnerability with telecom companies' infrastructure: At the same time that hackers and other cyber-criminals pose the threat of an attack, so do government agencies in their establishment of court surveillance. "Telecom companies are a big target for cyber-attacks because they build, control and operate critical infrastructure that is widely used to communicate and store large amounts of sensitive data," notes Deloitte.

The need for cybersecurity professionals and engineers in the telecommunications industry is wide-ranging, depending on the particular infrastructure and its challenges.

Key job responsibilities:

- Designing and maintaining cybersecurity systems and their architecture (especially where computer systems and devices communicate with one another)
- Developing procedures for detecting, defending against and responding to data breaches

- Troubleshooting network and infrastructure problems
- Understanding and complying with state and federal regulations

Prefered job requirements:
In addition to the CISSP, employers who have adopted an Information Security Management System (ISMS) may require an ISO/IEC 27001 certification, an international standard for managing and securing confidential data. Background checks, including fingerprinting and drug-screening, may be required.

Job examples:

- Cyber Incident Response Leader: Verizon in Ashburn, Virginia
- Cybersecurity Engineer: AT&T Corporate in Columbia, Maryland
- Executive Director of Product Security Technology: Comcast, Philadelphia

Career outlook:
Average salaries nationwide are from $91,000 – $119,000. From July 1, 2015 to June 30, 2016, Verizon alone posted 878 cybersecurity jobs, according to the Burning Glass Technology Cybersecurity Jobs report of 2015.

Personal Technology: Laptops, Tablets, Smartphones, and 'the Cloud'

Today, 78% of adults under age 30 have a personal laptop or desktop computer, and 86% own a smartphone, according to a recent Pew Research study. Close behind, 68% of all U.S. adults own smartphones, and 45% own tablets. It should be no surprise that privacy and cybersecurity concerns and jobs addressing them —have grown as fast as the technology.

"Anything [hackers] can choose to do, they can," said Matthew Solnik, a 28-year-old security consultant at Accuvant Inc., in an interview with the Wall Street Journal. That's because hackers understand how to manipulate others' computers, and your smartphone is basically a computer in your pocket, constantly hooked to the internet and filled with your contacts, photos, texts and browsing history.

The content on your smartphone or tablet also comes from different places. Some is installed by the phone's manufacturer, but every app installed by a consumer can come from a different company, and each consumer chooses what to store in 'the cloud,' the term for a nearly infinite network of computer servers. The pressure to design cybersecurity protection for devices that have open access to the internet —with simple or no password protection —is creating more demand than ever before.

Key job responsibilities:

- At the manufacturing level, cybersecurity experts and engineers must design systems that protect trade secrets, proprietary information, and research and data about the company's workforce.
- In the software and app development world, the ability to implement end-to-end encryption is vital. This need was showcased in 2015 as Apple refused to hack its own iPhone technology to aid the FBI investigation of mass shootings in San Bernardino, California.

Prefered job requirements:

- In-depth knowledge of cryptography
- Understanding of firewall creation
- Expert in Cisco ASA
- Cisco Nexus and IOs platforms
- Networking background in Controller Area Network (CAN) communication
- Internet Protocol (IP) networking and software development skills
- Working knowledge of IDA Pro (a diassembler and debugger), Whireshark (a network packet analyzer), OllyDbg (an x86 debugger) and Secure Development Lifecycle (SDL)

Job examples:

- Senior Cybersecurity Research Engineers: LG in Lincolnshire, Illinois
- Senior System Architect: AT&T in New York, New York
- System Security Engineers: Samsung in Austin, Texas
- Senior Network Security Engineers: Apple in Santa Clara Valley, California

Career outlook:
National salaries range from $97,000 – $120,000. *"Executive management and boards of directors are now recognizing that cybersecurity is not just a tech problem, it's a business problem,"* said Charlie Benway, executive director of the Advanced Cyber Security Center, in an interview with ComputerWorld. *"We're starting to see more executive-level emphasis on cybersecurity, more resources coming into cybersecurity, across all industry sectors. That has definitely increased the demand for cybersecurity folks."*

Retail Companies: Protecting Consumer Information

Due to their high visibility in our world —and the amount of personal and financial information that credit-card and debit-card holders give to their financial institutions —cyber attacks on large retail companies easily command the highest level of consumer attention. *"Chief Information Security Officers (CISO) have become more common on companies' senior leadership teams,"* says Retailing Today. *"They might be in even higher demand after the highly publicized data breaches at Target, Home Depot, Neiman Marcus and other companies in the past couple of years."*

Key job responsibilities:

- Must protect not only data, but also the bottom line (a publicized breach of a large retailer can easily harm the public's confidence in that retailer)
- Must be adept at collecting, analyzing and interpreting qualitative and quantitative data

- Understanding and using risk management techniques
- Handling customer problems relating to data security
- Designing and implementing protocols for disaster prevention and recovery
- Writing intelligence briefings for stakeholders

Prefered job requirements:

- Maintain status as a Certified Information Systems Auditor (CISA) or Certified Information Security Manager (CISM)
- You may be required to be proficient with Transact-Structured Query Language (T)SQL – a set of programming extensions connected to transactions that expand query language used by Microsoft and Sybase.

Job examples:

- Senior Security Program Managers: Amazon in Seattle, Washington
- Cyber Security Analysts: Walmart in Bentonville, Arkansas
- IT Security Analysts: Barnes & Noble, Nationwide

Career outlook:
National salary averages range from $81,000 – $126,000. The retail trade has one of the three fastest increases in demand for cybersecurity workers, according to Burning Glass Research.

Health Care: Hospitals, Insurance, and Health Care Management

With the migration of medical records from paper to digital format, the need for exceptional cybersecurity in the industries handling those records is critical. While the HIPPA (Health Insurance Portability and Accountability Act) law sets limits on who can see your private medical information, the computer systems in which that information is stored can still be vulnerable to a cyberattack. In 2015, Anthem, the second-largest health care insurer in the nation, was hacked, compromising a database of nearly **80 million people.**

"Cybersecurity vulnerabilities and intrusions pose risks for every hospital and its reputation," writes the American Hospital Association on its website. *"Hospitals can prepare and manage such risks by viewing cybersecurity not as a novel issue but rather by making it part of the hospital's existing governance, risk management and business continuity framework."*

Key job responsibilities:

- Supporting new cloud applications for electronic health records while designing a cybersecurity system that responds to both emerging and persistent threats
- Complying with HIPPA, FDA and other regulations
- Managing large workforces, vendors and business associates in terms of cybersecurity protocol
- Supporting consumer access through patient portals

"Second-largest health care insurer in the nation, was hacked, compromising a database of nearly **80 million people**"

Prefered job requirements:
Experience in the medical field is seen as a plus. Information security certifications may be required such as:

- (ISC)2: A nonprofit association that supports professionals with resources and experience to impove the cybersecurity landscape.
- GIAC: Consists of three certifications (General Security Essentials Certification or GSEC, Certified Intrusion Analyst or GCIA, and Certified Incident Handler or GCIH).
- ISACA: Offers training and certification in best practices for the information security industry.

Job examples:

- Cyber Threat Intelligence Analysts, Cyber Security Architects and Cyber Security Analysts: Kaiser Permanente in Oakland, California
- Chief Information Security Officer: New York City Health and Hospitals Corporation in New York, New York
- Manager of Cyber Security: Children's Healthcare of Atlanta
- Advisory Information Security Engineers: Blue Cross Blue Shield in Baton Rouge, Loisiana

Career outlook:
National salaries range from $96,000 – $120,000. The health care industry had one of the three fastest-growing increases in demand for cybersecurity workers and engineers over the last five years, an increase of **+121 percent**, according to Burning Glass.

Financial Companies: Banks, Brokers, Financial services, and Securities

The proliferation today of online transactions, which include everything from individual PayPal payments to bank statements and bill-paying, has made cybersecurity at financial institutions a critical responsibility.

The same technological advances that enable the management of mountains of confidential data and give consumers the ultimate in convenience can also put financial institutions "in the crosshairs" for cyberattacks, according to a Symantec white paper on Cyber Security for Financial Services. In May 2016, the chair of the Securities and Exchange Commission (SEC) told the Reuters Financial Regulation Summit that cybersecurity is the biggest risk facing Wall Street and the country's financial system.

Key job responsibilities:

- In-depth understanding about cybersecurity, risk analysis, and data science
- Engineering secure and robust systems
- Designing and testing security measures
- Nurturing a security-conscious culture of software developers

Prefered job requirements:

- Risk management experience
- Knowledge of state and federal legislation/ regulations
- Analytical and critical thinking skills
- Project management and research skills

- Understanding of geographic information systems (GIF) and strategic threat assessments

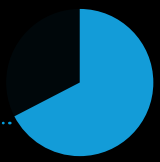
Job examples:

- Cyber investigations, intelligence and threat analysis, surveillance and data science, and security platform development and engineering: Goldman Sachs
- Cyberseurity engineer: Wells Fargo, Chandler, Arizona
- Cyber Security Assessment Coordinators: Bank of America in Simi Valley, California
- Principal Banking Risk Management Specialists: International Finance Corporation-Asset Management Company of the World Bank Group in Washington, D.C.
- Cyber Intelligence PII (Personal Identity Information) Consultants: Barclays in New York

Career outlook:
National salaries range from $110,000 – $129,000. Finance is one of the three industries (in addition to health care and retail trade) with the fastest increases in demand for cybersecurity workers, a 137% increase over the last 5 years according to Burning Glass Technologies' Cybersecurity Jobs Report.

"Percentage of CEOs that said they were concerned that cybersecurity threats could influence growth at the companies they run."

66%



Entertainment: Safeguarding Gaming Consoles and Peripherals

In 2014, a hacker group took over the computers of Sony Pictures and leaked confidential information about the companies' employees and families, including email and information about salaries. In April of 2016, a survey by PricewaterhouseCoopers of more than 1,400 entertainment and media CEOs said that **66%** of those executives are concerned that cybersecurity threats could influence growth at the companies they run. *"Today, financially motivated hackers are increasingly targeting the creative industry,"* says Sam Rastogi of Cisco, a 15-year security industry veteran.

Key job responsibilities:

- Creating strategy and protocol to assess, mitigate, and respond to threats
- Developing relationships with high-level domestic and international law enforcement
- Helping develop crisis management policy
- Monitoring, collecting, and analyzing networks of information
- Managing cybersecurity teams to improve outcomes

Prefered job requirements:
Along with a thorough understanding of gaming peripherals and networks, related certifications may be required such as:

- GIAC: Consists of three certifications (General Security Essentials Certification or GSEC, Certified Intrusion Analyst or GCIA, and Certified Incident Handler or GCIH).

- ISACA: Offers training and certification in best practices for the information security industry.

Job examples:

- Director of Global Intelligence and Threat Analysis: Disney Corporate in Burbank, California
- Director of Vulnerability Management Engineering: Sony in Washington, DC.
- Infastructure Engineer: Warner Bros. Entertainment Group in San Francisco, California
- Security Software Engineer: Sony Interactive Entertainment PlayStation in San Diego, California
- Manager of Global Product and Cyber Security: Nintendo of America in Redmond, Washington

Career outlook:
National salaries range from $96,000 – $110,000. In May of 2016, Information Week's Dark Reading revealed the high and underreported numbers of hacks of online gamers' personal information, citing one company that admitted to monthly hacks affecting 77,000 of its consumers. This means a significant increase in need for cybersecurity professionals to combat these issues.

Transportation: Roads, Travel, and Shipping

Any transportation system is only as strong as its weakest point, whether it means travel on interstates, airplanes, trains, or boats. Regulation and responsibility for cybersecurity often is shared between government entities the Department of Homeland Security, the Department of Transportation, and for-profit companies such as airlines, which also must protect ticketing operations and baggage handling.

In the case of international travel, cooperation between countries is paramount. *"It is critically important to secure every aspect of the transportation infrastructure and ensure that it remains open, operational, and — above all — safe for the billions of people who depend on it,"* says Parsons management security firm.

Key job responsibilities:

- Creating and managing cybersecurity baselines
- Understanding local, state and government regulations in your transportation sector
- Performing risk assessments and risk management
- Managing and training teams
- Developing threat prevention and response protocol
- Understanding and deploying data protection technologies

Prefered job requirements:

- Certified Information Security Manager (CISM) certification
- Global Information Assurance Certification (GIAC)

Job examples:

- Transportation Product Cybersecurity Engineering Managers: General Electric in Erie, Pennsylvania or Melbourne, Florida
- Network Security Administrator: Mitsubishi Electric U.S. Inc. in Warrendale, Pennsylvania
- Lead Cyber Security Analysts: Honeywell in Karnataka, India
- Senior Analysts in Cyber Security Intelligence: United Airlines in Chicago

Career outlook:
Salaries nationwide range from $99,000 – $147,000. The Burning Glass Cybersecurity Jobs Report of 2015 says that Air Transportation cybersecurity is one of the most quickly growing subsectors of professional services, with 221% growth in job postings between July 1, 2015 and June 30, 2016.

Government Agencies: Homeland Security and Department of Defense

The Department of Homeland Security (DHS) is widely considered the heart of cybersecurity analysis. In 2014, Bloomberg News reported that the Pentagon planned to triple its cybersecurity staff, and the FBI planned to hire 2,000 agents and analysts in its cyber division. The numbers would make 6,000 new "cyberwarriors" hired in two years.

The National Security Agency (NSA) offers rewarding career opportunities for cybersecurity experts and falls under the umbrella of the Department of Defense. The agency boasts exceptional employee benefits and respected career paths. In fact, the government-funded RAND Corporation notes, *"[The] NSA also has a very low turnover rate (losing no more to voluntary quits than to retirements. One reason is that it pays attention to senior technical development programs to ensure that employees stay current and engaged."*

Key job responsibilities:
The Department of Defense (DoD) has three prongs to its cyber strategy: to defend its own networks and information, to defend the U.S. homeland and its national interests, and to provide support to military operations. Other responsibilities include:

- Cyber incident response
- Cyber risk and strategic analysis, vulnerability detection and assessment
- Intelligence and investigation
- Networks and systems engineering
- Digital forensics and forensics analysis
- Software assurance training

Prefered job requirements:
In order to land cybersecurity or engineering leadership positions within the US government, you must obtain and keep a Top Secret security clearance and file a Public Financial Disclosure. Additonally, related certifications internships may be preferred, including:

- CISM Certified Information Security Manager
- NSA Summer Internships and Scholarships
- Department of Homeland Security Internship

Job examples:
Most, though not all, DHS jobs are in the Washington, D.C. area. Some top job opportunities for graduates include:

- Deputy Director
- Forensic Investigator
- Office of Cyber and Infrastructure Analysis
- Deputy Division Director in the Division of Electrical, Communications and Cyber Systems

The Department of Defense also offers Supervisory Information Technology Specialist positions for qualified graduates.

Career outlook:
Government salaries have a ladder and a scale; sample vacancies command salaries of $92,000 – $185,000. "As technology becomes increasingly more sophisticated, the demand for an experienced and qualified workforce to protect our Nation's networks and information systems has never been higher," says the Department of Homeland Security.

Military: Air Force, Army, Coast Guard, Marines, and Navy

"You are the first line of defense," states the United States Army Cyber Command and Second Army web page. The cyber command *"directs and conducts integrated electronic warfare, information and cyberspace operations as authorized, or directed, to ensure freedom of action in and through cyberspace and the information environment, and to deny the same to our adversaries."*

Key job responsibilities:

- Performing and leading information assurance activities
- Helping to plan, modify, and comply with cybersecurity policies and practices
- Serving as liaisons to higher commands and external cybersecurity agencies

Prefered job requirements:
Candidates must have either registered with or have been exempted from the Selective Service. In addition to CISSP certification, the DoD's Information Assurance Workplace certification (IAW) may be required.

Job examples:

- Information Technology Specialist as part of the U.S. Pacific Fleet: Navy/Marines at Naval Air Station in San Diego
- Information Technology Project Manager (Policy Planning): Army, Fairfield, California
- Intelligence Operations Specialist assigned to the Cyber Operations Squadrom: Air Force/Air National Guard in Boise, Idaho
- Raytheon Security Systems Engineer: Pascagoula, Missouri

Career outlook:
Salaries follow the government ladder and scale; averages run between $59,000 – $130,000. As recently as 2016, the DHS had been given authority to hire an additional 1,000 cyber professionals.

Overall, the outlook for jobs in cybersecurity is very bright. *"The big story in the cybersecurity labor force is a severe workforce shortage,"* says CSO's Cybersecurity Business Report. *"The demand for the (cybersecurity) workforce is expected to rise to 6 million (globally) by 2019, with a projected shortfall of 1.5 million,"* states Symantec CEO Michael Brown in the article.

Top 10 Companies in Cybersecurity Job Postings

In its "100 Best Jobs" rankings, U.S. News and World Report put Information Security Analyst jobs at No. 5 in Best Technology Jobs and No. 34 overall. The job market was scored as 10 out of 10, and the salary was scored at 7.5 out of 10.

Burning Glass Research Technologies' Cybersecurity Jobs 2015 report lists employers with the most job postings between July 1, 2015 and June 30, 2016. These are the companies at the top of the list, and the number of jobs they posted:

1. Oracle (software): 2,932
2. General Dynamics (aerospace defense): 2,083
3. Booz Allen Hamilton (government consultant in technology management): 1,143
4. Verizon Communications (telecommunications): 878
5. Mantech International (defense): 873
6. Wells Fargo (financial): 844
7. Northrop Grumman (global security): 820
8. Raytheon (aerospace/defense): 719
9. Deloitte (professional services): 704
10. Dell (computers): 653

How to Secure the Cybersecurity Job You Really Want

As in any industry, you're competing with other job candidates who may also have degrees and various levels of experience. But knowing your way around some common certifications, internships, and professional associations can give you an edge.

General Certifications

- GIAC Security Essentials: The GSE Security Expert (GSE) certification is widely considered the most prestigious in the information security industry. It consists of a multiple-choice test with a 3-hour time limit and a 2-day lab exam that includes an incident response scenario and multiple hands-on exercises. Prior to taking the GSE exam, you must successfully complete three GIAC certifications (General Security Essentials Certification or GSEC, Certified Intrusion Analyst or GCIA, and Certified Incident Handler or GCIH) and earn GIAC Gold for at least two of them.
- CISSP Certified Information Systems Security Professional: A certification that covers 8 primary domains: security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations and software development security. The exam is 6 hours long and covers 250 questions. The CISSP is required in many information security jobs.
- SSCP Systems Security Certified Practitioner: SSCP certification signifies your competency in access controls, security operations and administration, risk identification, monitoring and analysis, incident response and recovery, cryptography, network and communications security and systems, and application security. It is a 3-hour exam and covers 125 questions.
- CISM Certified Information Security Manager: CISM certification can mean career advancement and higher salary levels. It shows that you are competent in designing, managing, overseeing, and assessing information security programs, in addition to competence in the relationship between information technology and a company's wider goals. The exam takes about 4 hours and covers 200 questions.
- CISA Certified Information Systems Auditor: The CISA distinction signifies that you are in a more knowledgeable and more experienced group of information security peers. Candidates must pass the 4-hour, 200-question exam, agree to abide by a code of professional ethics, submit proof of five years of professional information security experience, and continue their professional education.
- CEH Certified Ethical Hacker: Being certified as an ethical hacker shows competency in understanding the weaknesses in information security systems to make them stronger. The 4-hour test covers 125 questions.
- ESCA EC-Council Certified Security Analyst: A next step after the CEH certification, this distinction shows that you understand how to interpret and analyze the results of using ethical hacking tools. The test takes 4 hours and covers 150 questions.

- CWSP Certified Wireless Security Professional: The CWSP certification focuses on WLAN security audits and network setups protected by intrusion systems. It shows competence in configuring security design and architecture and an understanding of the latest technologies available. The 90-minute test includes 60 questions.

Internships and Volunteering Opportunities

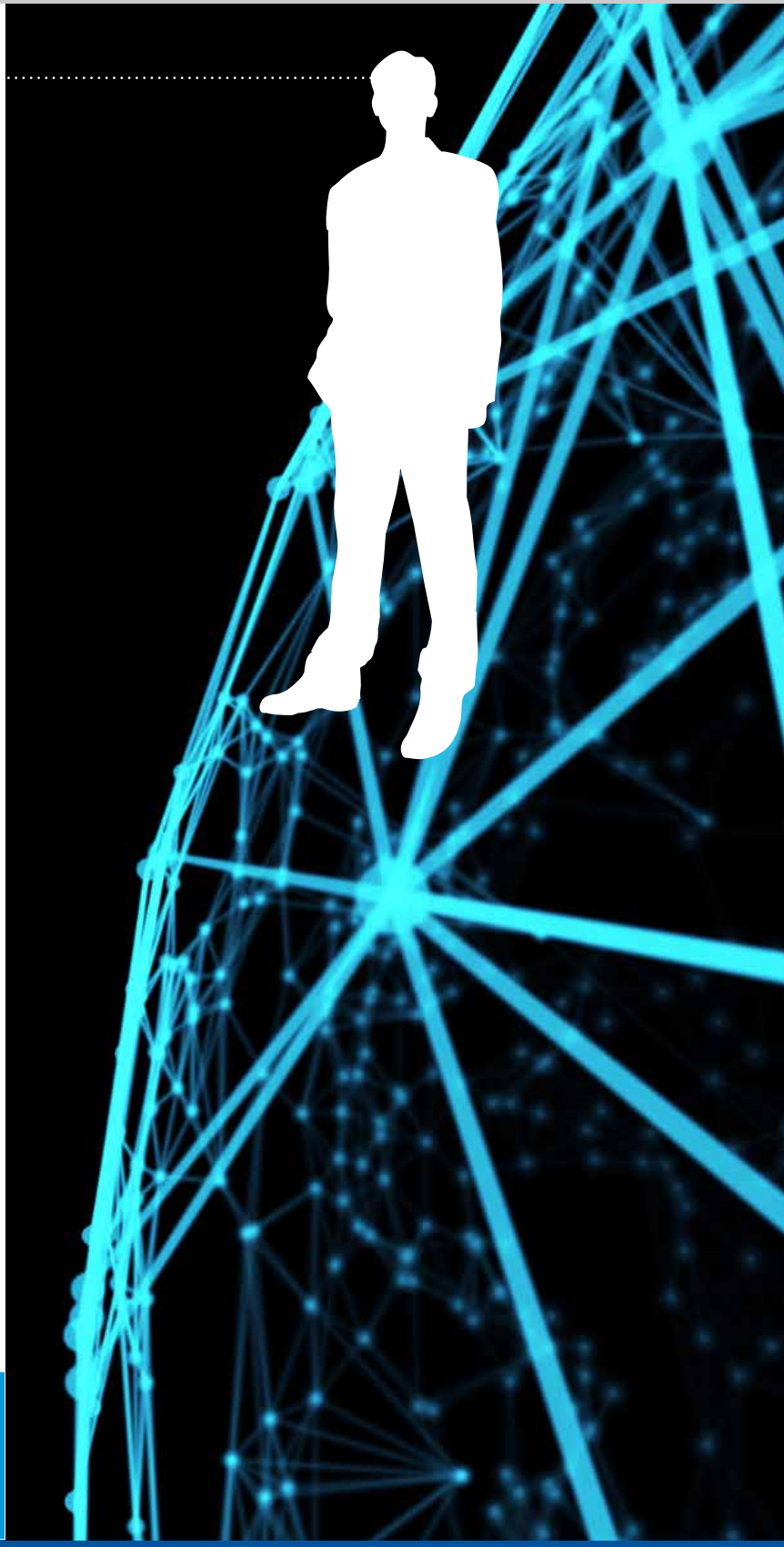
- NSA Summer Internships and Scholarships: NSA-based opportunities for high school, undergraduate, and graduate students from The Center for Cybersecurity Education and Research.
- Department of Homeland Security Cyber Student Volunteer Initiative: A DHS honors program in which 50+ undergraduate and graduate students receive volunteer assignments in field offices across the country, giving them experience and helping the DHS expand its cybersecurity workforce.
- Department of Homeland Security Internship: Ten-week internship opportunities for undergraduate and graduate students in which participants work alongside DHS professionals in cybersecurity-related research projects.
- NASA National Space Club Scholarships and Internships: Several annual scholarships and 50 summer internships at NASA facilities are offered to high school sophomores, juniors, and seniors.

Professional Organizations

- Association for Computing Machinery: Regarded as the world's largest educational and scientific computing society and focuses on advancing computing as both a science and a profession through publications, conferences, and other resources.
- Institute of Electrical and Electronics Engineers (IEEE): A professional organization dedicated to technological innovation and excellence. Its stated core purpose is to benefit humanity.
- National Society of Professional Engineers: A national organization that supports the concerns and livelihoods of professional engineers across all disciplines.
- Society of American Military Engineers (SAME): Dedicated to finding and resolving national security challenges that are infrastructure-related. In addition to engineers, participating professionals include architects, environmental and facility managers, and cybersecurity experts.
- Information Systems Audit and Control Association (ISACA): The organization that offers training and certification in best practices for the information security industry.
- Association of Information Technology Professionals: A global society of professionals in IT and IS fields. Chapter meetings, webinars, and conferences create networking opportunities for members, and a newsletter keeps members updated on industry trends.
- Information Systems Security Association (ISSA): An international association of information security professionals dedicated to managing technological risk and advancing the industry.

Resources and Tools Used by the Professionals

- SysInternals: A Windows website that hosts advanced system utilities and technical information.
- Windows GodMode: A hidden feature that allows a user to access all of an operating system's control panels from a single folder.
- Microsoft Enhanced Mitigation Emergency Toolkit (EMET): A utility that helps shore up vulnerabilities in software that could be exploited.
- Secure@Source: A program that analyzes and ranks risk of sensitive security data so organizations can better insure their security.
- IBM's Q-Radar: An IBM platform that integrates several aspects of information security management, including event management, log management and incident response, and forensics.
- HP's ArcSight: A program that manages data collection, storage, and analysis for security purposes.
- Splunk: Bills itself as the "leading platform for real-time operational intelligence," meaning that it is adept at searching, analyzing, and managing large amounts of IT and infrastructure data.
- Cyphort: Cyphort is a company focusing on next-generation solutions for malware in the form of Advanced Persistent Threats, or APTs.
- FireEye: A cybersecurity company that protects large and small companies against data breaches and cyberattacks.



Finding Your Place in the Cybersecurity Industry

"Cybercrime fueled a cybersecurity market explosion over the past five years, leading to one million cybersecurity job openings entering 2016. All signs point towards a prolonged cybersecurity workforce shortage through at least 2021" says Steve Morgan, founder and CEO at Cybersecurity Ventures.

How do you find your path in such a quickly growing and changing industry? How do you make the right choices to ensure future success?

If protecting our global digital infrastructure interests you, the University of Delaware's online Master of Science in Cybersecurity degree program can open doors whether you are new to the industry or hoping to advance or change your career. In fact, the National Security Agency and the Department of Homeland Security have designated the university a National Center of Academic Excellence in Cyber Defense Education. You will study with faculty members that come from corporate, government, and military sectors, learning both theory and real-life scenarios.

The 30-credit online program can be completed in as few as two years. In it, students advance through such classes as advanced cybersecurity, digital forensics, pen test and reverse engineering, secure software design and applied cryptography, learning:

- Cybersecurity fundamentals
- The engineering of secure software and systems
- How to apply theory to address modern cybersecurity issues
- The design and implementation of cybersecurity solutions
- How to address cyber attacks with local, national and global industries

For more information on the Master of Science in Cybersecurity program, call (302)-831-2405.