Information Security Analysts

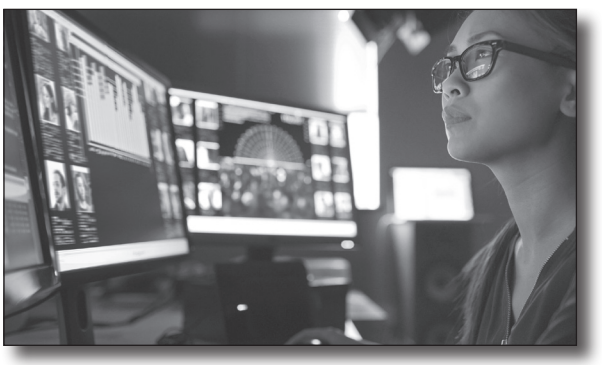
Snapshot

2017 Median Pay: $95,510 per year, $45.92 per hour
Typical Entry-Level Education: Bachelor's degree
Work Experience in a Related Occupation: Less than 5 years
On-the-job Training: None
Number of Jobs, 2016: 100,000
Job Outlook, 2016-26: 28% (Much faster than average)
Employment Change, 2016-26: 28,500

CAREER OVERVIEW

What Information Security Analysts Do

Information security analysts install software, such as firewalls, to protect computer networks. They work to protect a company's computer systems



Information security analysts plan and carry out security measures to protect an organization's computer networks and

systems. Their responsibilities are continually expanding as the number of cyberattacks increases.

Duties

Information security analysts typically do the following:

- Monitor their organization's networks for security breaches and investigate a violation when one occurs
- Install and use software, such as firewalls and data encryption programs, to protect sensitive information
- Prepare reports that document security breaches and the extent of the damage caused by the breaches
- Conduct penetration testing, which is when analysts simulate attacks to look for vulnerabilities in their systems before they can be exploited
- Research the latest information technology (IT) security trends
- Develop security standards and best practices for their organization
- Recommend security enhancements to management or senior IT staff
- Help computer users when they need to install or learn about new security products and procedures

IT security analysts are heavily involved with creating their organization's disaster recovery plan, a procedure that IT employees follow in case of emergency. These plans allow for the continued operation of an organization's IT department. The recovery plan includes preventive measures such as regularly copying and transferring data to an offsite location. It also involves plans to restore proper IT functioning after a disaster. Analysts continually test the steps in their recovery plans.

Information security analysts must stay up to date on IT security and on the latest methods attackers are using to infiltrate computer systems. Analysts need to research new security technology to decide what will most effectively protect their organization.

WORK ENVIRONMENT

Many analysts work in IT departments and manage the security of their companies computer networks.

Information security analysts held about 100,000 jobs in 2016. The largest employers of information security analysts were as follows:

Computer systems design and related services	28%
Finance and insurance	19
Management of companies and enterprises	9
Information	8
Administrative and support services	6

Many information security analysts work with other members of an information technology department, such as network administrators or computer systems analysts.

Work Schedules

Most information security analysts work full time. Information security analysts sometimes have to be on call outside of normal business hours in case of an emergency. About 1 in 4 worked more than 40 hours per week in 2016.

Fast Fact

Here are some worrisome numbers: 8 in 10 adults in the U.S. are concerned about businesses' ability to protect their financial and personal information, and cybercrime cost U.S. consumers $19.4 billion of their own money in 2017.

Source: American Institute of CPAs.

HOW TO BECOME AN INFORMATION SECURITY ANALYST

There are a number of information security certifications available, and many employers prefer candidates to have certification.

Most information security analyst positions require a bachelor's degree in a computer-related field. Employers usually prefer analysts to have experience in a related occupation.

Education

Information security analysts usually need at least a bachelor's degree in computer science, information assurance, programming, or a related field.

Some employers prefer applicants who have a Master of Business Administration (MBA) in information systems. Programs offering the MBA in information systems generally require 2 years of study beyond the undergraduate level and include both business and computer-related courses.

Work Experience in a Related Occupation

Information security analysts generally need to have previous experience in a related occupation. Many analysts have experience in an information technology department, often as a network or computer systems administrator. Some employers look for people who have already worked in fields related to the one in which they are hiring. For example, if the job opening is in database security, they may look for a database administrator. If they are hiring in systems security, a computer systems analyst may be an ideal candidate.

Licenses, Certifications, and Registrations

There are a number of information security certifications available, and many employers prefer candidates to have certification, which validates the knowledge and best practices required from information security analysts. Some are general information security certificates, such as the Certified Information Systems Security Professional (CISSP), while others have a more narrow focus, such as penetration testing or systems auditing.

ADVANCEMENT

Information security analysts can advance to become chief security officers or another type of computer and information systems manager.

Important Qualities

Analytical skills. Information security analysts must carefully study computer systems and networks and assess risks to determine how security policies and protocols can be improved.

Detail oriented. Because cyberattacks can be difficult to detect, information security analysts must pay careful attention to computer systems and watch for minor changes in performance.

Ingenuity. Information security analysts must anticipate information security risks and implement new ways to protect their organizations' computer systems and networks.

Problem-solving skills. Information security analysts must respond to security alerts and uncover and fix flaws in computer systems and networks.

WAGES

Median annual wages, May 2017

Information security analysts: $95,510

Computer occupations: $84,580

Total, all occupations: $37,690

Note: All Occupations includes all occupations in the U.S. Economy. Source: U.S. Bureau of Labor Statistics, Occupational Employment Statistics

The median annual wage for information security analysts was $95,510 in May 2017. The lowest 10 percent earned less than $55,560, and the highest 10 percent earned more than $153,090.

In May 2017, the median annual wages for information security analysts in the top industries in which they worked were as follows:

Computer systems design and related services	$98,100
Finance and insurance	97,680
Information	96,250
Administrative and support services	91,510
Management of companies and enterprises	90,940

Most information security analysts work full time. Information security analysts sometimes have to be on call outside of normal business hours in case of an emergency. About 1 in 4 worked more than 40 hours per week in 2016.

JOB OUTLOOK

Percent change in employment, projected 2016-26

Information security analysts: 28%

Computer occupations: 13%

Total, all occupations: 7%

Note: All Occupations includes all occupations in the U.S. Economy. Source: U.S. Bureau of Labor Statistics, Employment Projections program

Employment of information security analysts is projected to grow 28 percent from 2016 to 2026, much faster than the average for all occupations.

Demand for information security analysts is expected to be very high. Cyberattacks have grown in frequency, and analysts will be needed to come up with innovative solutions to prevent hackers from stealing critical information or creating problems for computer networks.

Banks and financial institutions, as well as other types of corporations, will need to increase their information security capabilities in the face of growing cybersecurity threats. In addition, as the healthcare industry expands its use of electronic medical records, ensuring patients' privacy and protecting personal data are becoming more important. More information security analysts are likely to be needed to create the safeguards that will satisfy patients' concerns.

Employment of information security analysts is projected to grow 56 percent in computer systems design and related services from 2016 to 2026. The increasing adoption of cloud services by small and medium-sized businesses and a rise in cybersecurity threats will create demand for managed security services providers in this industry.

Job Prospects

Job prospects for information security analysts should be good. Information security analysts with related work experience will have the best prospects. For example, an applicant with experience as a database administrator would have better prospects in database security than someone without that experience.

Employment projections data for Information Security Analysts, 2016-26

Occupational Title	SOC Code	Employment, 2016	Projected Employment, 2026	Change, 2016-26	
				Percent	Numeric
Information security analysts	15-1122	100,000	128,500	28	28,500

Source: Bureau of Labor Statistics, Employment Projections program

SIMILAR OCCUPATIONS

This table shows a list of occupations with job duties that are similar to those of information security analysts.

OCCUPATION	JOB DUTIES	ENTRY-LEVEL EDUCATION	2017 MEDIAN PAY
Computer and Information Research Scientists	Computer and information research scientists invent and design new approaches to computing technology and find innovative uses for existing technology. They study and solve complex problems in computing for business, medicine, science, and other fields.	Master's degree	$114,520
Computer and Information Systems Managers	Computer and information systems managers, often called information technology (IT) managers or IT project managers, plan, coordinate, and direct computer-related activities in an organization. They help determine the information technology goals of an organization and are responsible for implementing computer systems to meet those goals.	Bachelor's degree	$139,220
Computer Network Architects	Computer network architects design and build data communication networks, including local area networks (LANs), wide area networks (WANs), and Intranets. These networks range from small connections between two offices to next-generation networking capabilities such as a cloud infrastructure that serves multiple customers.	Bachelor's degree	$104,650

OCCUPATION	JOB DUTIES	ENTRY-LEVEL EDUCATION	2017 MEDIAN PAY
Computer Programmers	Computer programmers write and test code that allows computer applications and software programs to function properly. They turn the program designs created by software developers and engineers into instructions that a computer can follow.	Bachelor's degree	$82,240
Computer Support Specialists	Computer support specialists provide help and advice to computer users and organizations. These specialists either support computer networks or they provide technical assistance directly to computer users.	High school diploma or equivalent (some companies require associate's or bachelor's degree)	$52,810
Computer Systems Analysts	Computer systems analysts, sometimes called systems architects, study an organization's current computer systems and procedures, and design solutions to help the organization operate more efficiently and effectively. They bring business and information technology (IT) together by understanding the needs and limitations of both.	Bachelor's degree	$88,270
Database Administrators	Database administrators (DBAs) use specialized software to store and organize data, such as financial information and customer shipping records. They make sure that data are available to users and secure from unauthorized access.	Bachelor's degree	$87,020
Network and Computer Systems Administrators	Computer networks are critical parts of almost every organization. Network and computer systems administrators are responsible for the day-to-day operation of these networks.	Bachelor's degree	$81,100

OCCUPATION	JOB DUTIES	ENTRY-LEVEL EDUCATION	2017 MEDIAN PAY
Software Developers	Software developers are the creative minds behind computer programs. Some develop the applications that allow people to do specific tasks on a computer or another device. Others develop the underlying systems that run the devices or that control networks.	Bachelor's degree	$103,560
Web Developers	Web developers design and create websites. They are responsible for the look of the site. They are also responsible for the site's technical aspects, such as its performance and capacity, which are measures of a website's speed and how much traffic the site can handle. In addition, web developers may create content for the site.	Associate's degree	$67,990

Famous First

The Fourth Amendment to the U.S. Constitute alludes to the right to privacy. This amendment can be traced back to English legal doctrine. In Semayne's case (1604), Sir Edward Coke stated: "The house of every one is to him as his castle and fortress, as well for his defence against injury and violence as for his repose." Semayne's Case acknowledged that the King did not have unrestricted authority to intrude on his subjects' dwellings, but did establish that government agents could conduct searches and seizures when their purpose was lawful and a warrant had been obtained.

Source: https://en.wikipedia.org/wiki/Fourth_Amendment_to_the_United_States_Constitution

Conversation With . . .
RYDER JEFFERSON MOSES

Vice President of Information Security
Electronic Payment Processor, Mid-Atlantic Region
IT, 32 years; Cybersecurity, 5 years

1. What was your individual career path in terms of education/training, entry-level job, or other significant opportunity?

I graduated with a biology degree in 1981 to limited employment opportunities, so I fixed computers and printers because I have good mechanical aptitude. I realized that what really grabbed my attention was networks, data transmission, and telecommunications carrier services between computers. This was before the internet. As my career in network engineering progressed, I experienced, first-hand, the evolution of data transmission protocols for both private and public (internet) networks.

I wound up working as a contractor on government networks, and decided to go back to school so I had the academic credentials to back up the work I'd been doing for 10 years. I got my master's in Telecommunications Management; today I would recommend a degree in information security, which wasn't available at that time.

I went on to work for a company that supports banks in the electronic payment processing industry. As that business grew—dramatically—and credit card processing migrated toward the internet, it became vulnerable to hackers who stole information to produce counterfeit credit cards. This was in the early 2000s, and the increased use of the internet gave rise to new encryption methods for data transmission. As I spent more time implementing encryption methods, I was working closely with people in the developing field of information security.

As encryption grew more sophisticated, the hackers became more sophisticated at uncovering vulnerabilities, which led to the creation of a security standard to force banks, merchants, and processors to improve data protection methods. In my most recent role, I helped explain to merchants the need to implement these measures to meet the Payment Card Industry Data Security Standards. I also helped merchants make changes to support chip-enabled payment cards.

2. What are the most important skills and/or qualities for someone in your profession?

Critical thinking skills, an analytical approach to risk assessment, and a fundamental understanding of cryptography and data transmissions protocols, because you need

the ability to do an end-to-end assessment of the data processing environment. Also, you need a clean background check with no arrests and an absolute dedication to integrity. You aren't going to get a join information security if potential employers have any reason to suspect they can't trust you.

3. What do you wish you had known going into this profession?

The fact that you will be on call 24/7, 365 days because you need to drop whatever you're doing and devote all your attention to any kind of data compromise. I once left a company meeting to help decode transaction data in real time after a guy who'd just gotten out of jail for committing credit card fraud stole a dial-up terminal and started doing fraudulent credit card transactions from his house. I was on a conference call with law enforcement sitting in a van across from his house as I manually decoded his fraudulent transactions so they could catch him in the act.

4. Are there many job opportunities in your profession? In what specific areas?

Definitely. Every merchant who accepts credit and debit cards needs technical personnel to assess vulnerabilities and implement measures to protect themselves, the cardholders, and the banks. Many industries face growing information security requirements, including banks, electronic funds processing companies, stock brokerages, hospitals, government agencies, and colleges.

5. How do you see your profession changing in the next five years, and what skills will be required?

In this business, the technology—and the use of technology by the bad guys—evolves at a rapid pace. You have to constantly update your knowledge and skills, and continuously monitor systems and networks for emerging trends in vulnerability exploitation.

6. What do you enjoy most about your job? What do you enjoy least about your job?

I enjoy the satisfaction of knowing I'm helping to protect financial data and reduce the risk of financial losses to cardholders, merchants, and banks. I also enjoy explaining very technical security requirements in terms that everyone can understand. This field pays well, and I enjoy that.

I don't like being on call. I don't like security breaches, and the stress levels associated with protecting the country's commerce infrastructure while knowing that information security is only effective until the bad guys find another vulnerability to exploit.

7. Can you suggest a valuable "try this" for students considering a career in your profession?

Internships are a great way to learn about networks and data transmission technologies. There's also, certainly, a lot of information online. Look into things like Cisco router training. Also, the military is worth considering because they have training opportunities due to the critical requirements for keeping data secure.

This conversation was originally published in Careers in Information Technology *(Salem) 2016.*

Conversation With . . .
GREGORY WHITE, PhD

Cybersecurity director, 15 years

Gregory White is the director of the Center for Infrastructure Assurance and Security for the University of Texas in San Antonio, Texas.

1. What was your individual career path in terms of education/training, entry-level job, or other significant opportunity?

When I went to Brigham Young University (BYU) in Provo, Utah, I thought I was going to be a medical doctor. This had been my thought since middle school, even though my father had taught me FORTRAN on an old teletype machine back in fifth grade. He was rooting for computer science because he knew I liked it.

At BYU, I was automatically put into the pre-med chemistry track. It turned out chemistry and I did not get along. At age seventeen, away from home for the first time, I did not realize I could switch to a microbiology track because I did not talk to an academic advisor. I changed majors two more times before I ended up going into computer programming and earning a bachelor of science in computer science. It turned out my father was right.

An ROTC scholarship paid for my last two years of college. I entered the Air Force upon graduation and, after four years doing computer programming, they sent me to get a master's degree in computer engineering at the Air Force Institute of Technology in Dayton, Ohio. My thesis was on artificial intelligence and war gaming. I was then sent to San Antonio where the Air Force was forming a new computer security office.

At the time I went into computer security professionally, the internet was starting to appear. IBM personal computers had been introduced a few years earlier and people wanted to connect to others. The Air Force understood that its rules and regulations did not cover this new environment and intelligence sources were taking advantage of it.

The Morris Worm brought the Internet to its knees in 1988. After that, the people who tried to respond had a big meeting and from that came the computer emergency response team concept. I worked in the network security branch of the Air Force Cryptologic Support Center, which was part of the Air Force Electronic Security Command. I went on to advanced computer communication officer school, then to

teach at the Air Force Academy where I helped introduce security into the curriculum. After a few years, the Air Force sent me for a PhD in computer science at Texas A&M. My dissertation was in security intrusion detection. I went back to the academy and was responsible for creating its first undergraduate information warfare lab.

After nineteen years, I separated from the Air Force and went into the reserves. An opportunity had arisen to work in San Antonio with colleagues who created SecureLogix, Corp. I was vice president of services and chief technical officer there, and I also began teaching at UT San Antonio. An effort was underway to establish a cybersecurity program here. I came to the university fulltime in the fall of 2001.

Some of the things we are trying to teach people today are the same things we were trying to convince folks of twenty or more years ago. The natural thing for a computer scientist to do is to look at the problem of cybersecurity from a technical standpoint—all you need to do is build a secure system—but it's not just a technical problem.

Security is prevention, detection, and response. You have to assume the attackers are going to try to get in and it is critical to detect and respond. Our center has a big focus on helping communities and small and medium businesses understand what they need to be doing. That's a weak link. I guarantee there's a utility company somewhere in this country that is not protected.

On the education side, we have to start a culture of security. When I grew up, we knew that Smokey wanted us to prevent fires and McGruff told me to take a bite out of crime. Nobody is telling kids to take a bite out of cybercrime.

2. What are the most important skills and/or qualities for someone in your profession?

Intellectual curiosity. Someone who takes apart the phone. Bonus points if you can get it back together and it works. I need someone who says, "I wonder what would happen if…?"

3. What do you wish you had known going into this position?

This is not a job where you are going to get a degree and rest on your laurels. This field changes very quickly.

4. Are there many job opportunities in your profession? In what specific areas?

Many. The estimate of open security positions by 2023, depending on what study you read, ranges from a few hundred thousand to two million. Those are unfilled positions worldwide.

5. How do you see your profession changing in the next five years? How will technology impact that change, and what skills will be required?

Any time new technology is introduced you have to be on top of it because there will be security flaws and issues. It takes a lot of time; you must constantly read, go to conferences, and take classes. This will continue. Here at my center, we believe that we do not just need a larger security workforce; we need security in the workforce. Everybody needs to know his or her responsibilities.

6. What do you enjoy most about your job? What do you enjoy least about your job?

I like it because it does not get boring. There are times when it would be nice to slow down a little.

7. Can you suggest a valuable "try this" for students considering a career in your profession?

We produce something here called Cyber Threat Defender, designed to give people a basic understanding of cybersecurity. Find it at cyberthreatdefender.com. I also would encourage middle or high school students to participate in the CyberPatriot competition, which you can learn about at uscyberpatriot.org.

MORE INFORMATION

For more information about computer careers, visit

Association for Computing Machinery
https://www.acm.org/

Computing Research Association
https://cra.org/

IEEE Computer Society
https://www.computer.org/

For information about opportunities for women pursuing information technology careers, visit

National Center for Women & Information Technology
https://www.ncwit.org/

Sources

Bureau of Labor Statistics, U.S. Department of Labor, *Occupational Outlook Handbook*, Information Security Analysts.