Making Everything Easier!™

Getting an Information Security Job

FOR DUMMIES®

A Wiley Brand

Learn to:

- Identify information security roles
- Determine which certifications you need
- Write an attention-getting resume
- Prepare for interviews

Get access to free online resources, including video, articles, sample resumes, and more

Peter H. Gregory
CISSP, CISA, CRISC

Getting an Information Security Job

FOR DUMMIES®

A Wiley Brand

by Peter H. Gregory

FOR DUMMIES®

A Wiley Brand

Getting an Information Security Job For Dummies®

Published by: **John Wiley & Sons, Inc.,** 111 River Street, Hoboken, NJ 07030-5774, www.wiley.com

Library of Congress Control Number: 2014954662

ISBN 978-1-119-00281-9 (pbk) 978-1-119-00284-0 (ebk); ISBN 978-1-119-00262-8 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Table of Contents

Introduction

The information security (InfoSec) profession got its start decades ago, but it consisted of few people, mostly in military and other secret organizations. With the appearance of the Internet in the 1990s, organizations started to put information online, and the InfoSec profession became a little more popular. Fast-forward to the mid 2010s, with its big security breaches as well as new laws and regulations, and information security is one of the hottest professions around the world.

About This Book

There are more than enough books on information security, but far too few professionals to do the work. Until now, there was no clear guide to getting into the profession. Delivered in the same rich tradition of the *Dummies* series, *Getting an Information Security Job For Dummies* is that clear guide on planning your entry in information security, no matter where you are in your career today:

- **If you're a student or recent graduate,** you'll get real-life information on what it's like in the information security profession.
- **If you're an experienced IT professional,** you'll understand how to make a lateral move into information security.
- **If you're already getting your start in information security,** you can chart your career path and decide what kind of an organization you may want to work in.
- **If you're in the information security job market,** you'll understand different types of information security jobs in different types of organizations.
- **If you need to hire an information security professional,** you'll find lots of information to help you focus on what kind of candidate you need and to better understand the people who are applying for your positions.

No matter why you're reading this book, you can use it as a security career reference. *Getting an Information Security Job For Dummies* is full of insight from real information security professionals, in their own voices. You'll begin to understand what the InfoSec profession is really like from professionals who have been going at it for years.

Foolish Assumptions

While writing this book, I've made some assumptions about you:

- You are curious about technology and how things work. Even if you're looking to get into the compliance or controls aspect of information security, it's still important to have a healthy appreciation for how technology supports an organization.
- You dislike malware and the criminal organizations that create them. Even if you don't yet understand how cybercriminals work, your conscience tells you that what they are doing is wrong, and you want to learn how to help organizations better defend themselves.
- You enjoy learning. My first clue: You are reading this book! Being in information security — or any branch of information technology — demands continuous learning. Security issues and technology itself change quite rapidly, and continuous learning is needed just to keep up!
- You like Dr. Who and his problem-solving capabilities, even if some of the scenarios he finds himself in are a little odd.

How am I doing so far? If all of my assumptions are right, you may be InfoSec material and ready to seriously consider a career in information security.

Icons Used in This Book

Throughout this book, you'll see icons in the left margin that call attention to information that's worth noting. No smiley faces winking at you or any other cute little emoticons, but you'll definitely want to take note! Here's what to look for and what to expect.

Throughout the book, you'll find stories and tips from information security professionals, in their own voices.

This icon identifies general information and core concepts that are well worth committing to your nonvolatile memory, your gray matter, or your noggin' — along with anniversaries, birthdays, and other important stuff!

Thank you for reading; we hope you enjoy the book; please take care of your writers! Seriously, this icon includes helpful suggestions and tidbits of useful information that may save you some time and headaches.

Whatever I'm warning you about is nothing *that* hazardous. These helpful alerts point out easily confused or difficult-to-understand terms and concepts.

Beyond the Book

In additional to the material in the print or ebook you're reading, this product also comes with more online goodies:

- **Cheat sheet:** The cheat sheet offers tips on interviewing for an information security job and building your personal brand. You can find the cheat sheet at `www.dummies.com/cheatsheet/gettinganinformationsecurityjob`.
- **Web extras:** You'll find some great references that you can use, including a resume template, a sample resume, and a list of websites of value to information security professionals. Go to `www.dummies.com/extras/gettinganinformationsecurityjob`.
- Updates to this book, if we have any, are at `www.dummies.com/go/gettinganinformationsecurityjobudupdates`.

Where to Go from Here

If you're wondering what the information security profession is all about, go to Part I. If you want to dive into the education, training, and knowledge required in information security, start with Part II. If you're wondering what life is like in different types of organizations, Part III was written just for you. If you're ready to get out there in the InfoSec job market, go right to Part IV. If you love lists, head for Part V.

And for those who want to take an even deeper dive into the knowledge expected of information security professionals, get a copy of *CISSP For Dummies*, by Lawrence Miller and Peter H. Gregory.

Part I

So You Want to Be an InfoSec Professional

Visit www.dummies.com for great *For Dummies* content online.

In this part . . .

- Find out how industry conditions have led to today's high demand for skilled information security professionals.
- Understand typical job titles and their duties.
- Discover the security problems that governments and industries face today.

Chapter 1

Securing Your Future in Information Security

In This Chapter

- Understanding the need for information security professionals
- Reviewing a history of cybercrime

According to the *Cisco 2014 Annual Security Report*, the worldwide shortage of information security professionals exceeds *one million workers*. You have chosen a great time to learn more about this exciting and rapidly changing field!

This chapter takes a closer look at the changes in business and technology that have given rise to the high demand for information security workers. You also discover why information security is a great career field.

Why Does Information Security Matter?

Information security, or *InfoSec,* was once considered a technical discipline with little business relevance. Now, however, it is a topic of heated discussions in corporate boardrooms around the world. Information security matters because information technology matters — and because criminals are finding it easy to steal sensitive and private information from organizations' information systems.

Increased reliance on information systems

Organizations of every kind, as well as a growing number of private citizens, rely on information systems for conducting daily affairs more than ever before. We buy more and more Internet-connected products, partly for

convenience and partly for the cool factor. Before long, it will be easier to count the things that *aren't* connected to the Internet.

You might have heard that data and information are the new currency. Although this statement might sound like a cliche, it's true for several reasons:

- Organizations can use software tools to examine electronic business records and gain valuable insights that help them find new opportunities. For instance, a grocery store can add new items to its inventory based on sales trends.
- Organizations can use information systems to make business processes more efficient. For example, if an organization puts sales details in an information system, the customer service department could electronically access those records and be far more efficient.
- For banks and other financial institutions, data actually *is* money, or at least the closest representation of money. For instance, transferring funds or paying bills online is mostly about making a number bigger in one place and smaller in another.

This increased reliance on Internet-connected systems and devices makes our businesses more efficient and our lives easier, but there is a dark side: Criminals are also turning to Internet-connected systems to disrupt businesses and steal valuable information.

Growth in cybercrime

Organizations of every kind are increasing their reliance on information systems for storing and processing valuable information. Meanwhile, cybercriminal organizations have grown, organized, and made vast improvements in the skills and tools they use to find and steal this information.

"Last year was the first year that proceeds from cybercrime were greater than proceeds from the sale of illegal drugs, and that was, I believe, over $105 billion," according to Valerie McNiven, who advises the U.S. Treasury on cybercrime. "Cybercrime is moving at such a high speed that law enforcement cannot catch up with it." Ms. McNiven made this claim in 2005; in the past ten years, cybercriminal organizations have made impressive gains in their capability to steal valuable data.

According to idtheftcenter.org, some of the largest security breaches in 2014 were as follows:

- Sony Pictures: 33 thousand documents and several unreleased films
- U.S. Weather System: breach to NOAA weather satellite network

- JP Morgan Chase: 76 million records
- Home Depot: 56 million records
- Community Health Systems/Tennova: 4.5 million records
- Michaels Stores: 2.6 million records
- Texas Health and Human Services: 2 million records
- Internal Revenue Service: 1.4 million records
- Staples: more than 1.1 million records
- Neiman Marcus: 1.1 million records
- State of Montana: more than 1 million records
- Viator: 880 thousand records
- Goodwill Industries: 868 thousand records
- Oregon Employment Department: 851 thousand records
- U.S. Postal Service: 800 thousand records
- Variable Annuity Life Insurance Company: 774 thousand records
- Spec: 550 thousand records
- Aaron Brothers: 400 thousand records

Although 2014 was not an encouraging year in information security, it is for businesses whose mission is the protection of critical information.

So many security breaches are occurring that several websites are devoted to listing them, including

- `www.privacyrights.org`
- `www.idtheftcenter.org`
- `www.datalossdb.org`

Improved defenses

This scourge of break-ins and breaches does not mean that governments and industries are going to turn tail and stop their expansion of information systems. Instead, organizations of every size and type are hiring security professionals to improve security measures that protect their systems. Security professionals are doing the following to protect critical data:

- Hardening systems and applications to make them more difficult to attack
- Adding layers of defense

- Performing security scans to find vulnerabilities
- Conducting internal audits of security controls
- Training personnel to recognize intrusion attempts
- Improving security in partner and supplier organizations
- Updating business processes to include security procedures

A Brief History of Cybercrime

As far back as recorded history goes, we know that whenever one party collects or creates anything of wealth, another party will do his or her best to steal or spoil the owner's wealth. It makes sense, then, that as individuals and organizations use information systems to create, store, or spend wealth, others will do whatever they can to take the wealth for themselves. As individuals and organizations become increasingly reliant on information systems, more valuable information is created. So news of security breaches in which these information hordes are stolen or vandalized should not come as a surprise.

It helps to wind the clock back a few years to see how security breaches all came about. Although the first security incidents weren't so much about stealing money, they provided the foundation for later incidents in which monetary theft *was* the object.

The history of cybercrime can be thought of as two different related trends on a collision course:

- Improvements in malware potency
- Increased use of computers, networks, and the Internet to manage and control just about everything

These trends have gradually moved toward each other, each gaining momentum. If you're imagining two locomotives barreling toward each other, that's not quite the right image. The collision of malware potency and increased computer dependence has been slower — like cold air from the north colliding with warm air from the south, wreaking unpredictable havoc in multiple locations.

Malware

Malware is a general term that encompasses many kinds of harmful programs or program fragments such as viruses, Trojan horses, worms, and bots (for a more detailed description of malware, see Chapter 3). Early forms of malware

were simple, almost like experiments developed by computer hobbyists who thought, "I wonder what will happen if I build a piece of computer code that does this?"

These early versions of malware were crude and performed simple functions, such as displaying something on the computer screen or deleting files. The creators of malware made no attempt to hide themselves, because there was nothing to hide from.

Fast-forward to today, when malware has become so potent and stealthy that your life can become miserable if you depend on computers and networks.

Break-ins and breaches

Malware is not the only tool in an attacker's toolbox. Just as a lock-picking set is only one way to break into a building, other techniques are frequently used to break into computer systems, such as computer break-ins and breaches. Some of the techniques used include social engineering, phishing, and watering hole attacks. These attacks are occurring more often than before for a variety of reasons:

- More companies using information systems
- More companies are building interconnections
- Higher value information being stored on information systems
- Growing shortage of personnel who know how to implement good security
- Cybercriminal organizations building better intrusion tools
- Profitable cooperation among cybercriminal organizations

We are living in a perfect storm, where more companies are storing high-value information that they don't know how to protect from criminal organizations that are getting better at finding and stealing it. The situation is truly becoming dire, and we could use more help!

One of the biggest problems in computer security today is social engineering, which is any of several techniques of deception designed to take over computers or obtain sensitive information. When organizations do a good job of protecting their computers and networks, intruders turn to hacking people instead — too often with great success.

Fraud

Another form of cybercrime is online fraud. The definitions of *fraud*, according to Wiktionary, are

- Any act of deception carried out for the purpose of unfair, undeserved and/or unlawful gain.
- The assumption of a false identity to such deceptive end.
- A person who performs any such trick.

Fraud has been a problem since the beginning of history. And today, fraud has found a cozy home in the world of information systems and the Internet.

The most prevalent form of fraud is the *phishing scheme,* in which an adversary creates some ruse, identifies potential victims, and attempts to trick them into doing something they should not do. Here are some examples of email or other communications that the potential victim might receive:

- **Bank:** Your funds are low, or are being locked because of suspected fraud (this one's really ironic).
- **Taxes:** You owe taxes to the government and will be in trouble unless you pay right now.
- **Law enforcement:** You have overdue fines or there's a warrant for your arrest.
- **Sweepstakes:** You're the winner of a sweepstakes and must provide financial information to claim your prize.
- **Inheritance:** You have inherited money, and the organization that holds your funds needs help so that they can transfer your newfound wealth to you.
- **Friend in need:** A friend of yours is in trouble with law enforcement and needs you to send money to get out of jail.
- **Email account:** You need to confirm your identity and increase your storage to continue using your email account.

In these and virtually all others ruses, you think that you've been directed to the organization's website for the purpose stated, but you are actually sent to an imposter site. There, you might fill in your login credentials, which the fraudsters use to gain access to the real site and carry out their scheme, such as stealing your money or taking over your email account. Or the imposter

site has a form that requests a credit card number, a bank account number, or other sensitive information that the fraudster can use to separate you from your money.

Today's online fraud schemes are nothing more than modern-day confidence tricks designed to convince you to trust an unknown party and then provide them with sensitive information.

Knowing Your Adversaries

Many technologists think that an information security program is all about technology: That technology is the root of the problem and technology will solve those problems. If this describes you, I appeal to you to open your mind to other ways of thinking about information security. Even if the aspect of information security that fascinates you the most is technology (and we need a lot more people like you), understanding the people behind technology-related issues can be helpful.

Information security involves a lot of technology but is at its root a people issue. Information security professionals are responsible for protecting assets against people: careless insiders, malicious outsiders, and many in between. Our vocabulary includes a lot of terms for things, including the different sorts of actors and their unique behaviors that we all eschew. I describe them in this section.

Hobbyists and enthusiasts

Because the term *hacker* has been maligned in recent years, I prefer to use the term *computer hobbyist* to describe computer enthusiasts who love to explore computers to understand more about how they work. Hackers, hobbyists, and enthusiasts — let's agree that they're all about the same.

Hobbyists are curious, peaceful folk who love technology, love to figure out how things work, and love to improve their electronic gadgets. Hobbyists and inventors are similar. Both enjoy making things better for themselves and others by taking things apart (logically or literally) to see how they work, and then modifying them to make them better. The world is full of people who like to tinker with their cars, motorcycles, radios, and computers. Think of early computer overclockers or musicians whose amps go up to 11.

Hobbyists with good judgment and discipline are our friends.

The fall of hackerdom

Before most people in the world were even born, the term *hacker* was generally a positive one. A hacker was a hobbyist who was curious about how electronic-ish things worked and would implement customizations to improve or enhance their performance. In the early days of computers, a *computer hacker* was one who sought to understand how computers worked and to employ changes to improve them.

Then as now, some hackers would explore computer systems — still seeking how they worked and ways of making modifications — but for malicious purposes.

The term *hacker* as a benevolent hobbyist has fallen into disuse and the dominant meaning of the term is a malicious person. And good hackers are generally known as computer hobbyists so they can distance themselves from the others.

Script kiddies

A deservedly maligned bunch, *script kiddies* are teenage troublemakers with too much time on their hands who use tools created by others to attack computers and networks. Typical script kiddies have little or no understanding of the inner workings of the tools they use.

Early in my career, script kiddies were typically the most significant problem for us — there were a lot of them and the tools they used could cause quite a bit of damage. But in retrospect, they were like gnats that swarmed around our faces, irritating and bothersome but usually not very harmful.

Like a lot of technologists, some script kiddies start as novices but build their knowledge and skills. They improve the tools they use and, eventually, write hacking tools of their own.

Hacktivists

Hackivist is a blend of the words *hacker* and *activist* (think Greenpeace or PETA). Hacktivists are generally known for disrupting computers and networks belonging to organizations and governments with whom they disagree politically or ideologically.

It's a big crowded world, and the Internet is a never-ending fount of information about every sort of organization. For every organization, you'll likely find people who oppose what the organization does or stands for.

Some noteworthy examples of hacktivist activities follow:

- **PGP (pretty good privacy):** A popular email encryption program, PGP was thought to be released in response to a U.S. Senate bill that demanded government access to the plain text contents of voice, data, and other communications.
- **Website mirroring:** When an organization or a government blocks access to a particular website, a hacktivist will mirror (copy) the contents of the blocked site to another site, so that its contents can remain available.
- **Wikileaks:** This website publishes leaked industry and government documents.

Corporate spies

Companies spying on each other to obtain commercial secrets is nothing new. However, the migration of paper records to computers and the Internet has provided new opportunities and methods for companies to spy on each other. The Internet provides the means for spies to discover target systems and to steal their data for further analysis and exploitation.

The future is bright for information security jobs

There is a critical worldwide shortage of workers with information security skills. For the most part, these jobs pay well, with pretty good working conditions and a good standard of living.

In January 2014, the Ponemon Institute conducted a survey of information security managers and developed several key findings, including:

- 70 percent of respondents said that they don't have enough IT security staff.
- 58 percent of senior security staff positions and 36 percent of staff security positions went unfilled in 2013.

In 2014, Burning Glass Technologies market overview on information security jobs cited that job listings in cybersecurity have grown by 74 percent from 2007–2013, more than twice the growth rate for IT jobs overall.

Unlike the dot com bubble in the late 1990s, the growth rate in information security jobs is not a flash in the pan but a response to painful advances by cybercriminal organizations as well as increasing regulation on information security and privacy. Short of a miraculous discovery in data protection that cybercriminal organizations are unable to overcome (yeah, right!), the demand for information security jobs should remain strong for many years.

Malicious insiders

Take good care of your employees and they'll take good care of you. However, companies that don't treat employees so nicely sometimes pay a heavy price. Employees who are bored, angry, unhappy, or who think that they will soon be fired or laid off often use revenge to settle the score.

Now and then, we hear a tale in which an employee who believed that his or her job was about to end decided to exact revenge on the employer. The popular cult movie *Office Space* explores this theme in detail.

Careless insiders

A *careless insider* is a legitimate user in an organization but, well, careless. Perhaps the person lacks judgment, or is working too fast, or needs training, or is not paying attention.

Careless insiders can be especially damaging to an organization because they possess what intruders lack: issued login credentials.

Fraudsters

Fraudster is a broad label that includes people who deceive and steal. How they deceive and what they steal varies, but invariably they perform some kind of a trick to steal money.

Typical fraud cases in the broad category of cybercrime include the following:

- **Credit card fraud:** Fraudsters steal credit card numbers and use them to buy stuff they want. You might still get the frequent flyer miles or other rewards, but you're out the money, and that hurts.
- **Wire fraud:** Fraudsters employ malware that steals login credentials, and target a company with lots of money in the bank, in hopes that they can capture online banking and online wire transfer login codes. If they do, that giant sucking sound is the organization's money being transferred to an offshore account.
- **Identity theft:** These actors use a variety of ways to obtain enough personal information about people to permit the opening of credit cards and lines of credit in the name of the victim. (By the way, they aren't actually stealing your identity; they're borrowing it.)

Organized crime

Organized crime used to be known for sex and drug trafficking, illegal gambling, and protection rackets. Today, however, organized crime makes more money perpetrating online fraud and other Internet-based schemes. These organizations are in all corners of the world, but particularly in Eastern Europe, the Middle East, and Africa.

The sophistication of a lot of today's malware points to organizations with large, formal research and development budgets. Most of the easy hacks have been written; now more work (and bigger organizations) and better planning are required to build the tools necessary to break into systems and networks.

Rogue nation-states

The governments of several countries understand that state sponsorship is one way to develop malware and other techniques to break into networks and steal valuable information.

Nation-states sponsor cybercriminal activities for a number of reasons, such as to

- Steal political secrets
- Steal military secrets
- Aid local industries through industrial espionage
- Conduct industrial or military sabotage

If this sounds like traditional espionage — you're right! Today's spies have moved into cyberspace to do their work. If the information they want is online, many will use online means to try and steal it.

Cyberwarfare rules of engagement

If you're on the side of the white hats, cyberwarfare is not a lot of fun. If it seems like adversaries have the upper hand, it's because adversaries have the upper hand.

Cyberware is said to be asymmetric. In other words, a single individual can wield the same amount of attack effectiveness as the largest country in the world. With the right tools, an individual can cripple a large military organization.

The following lists some rules of engagement for attackers and defenders:

- Defenders must protect against all types of attacks, whereas an attacker can attack in any manner desired.
- Defenders must protect all systems against attack, whereas an attacker can attack any system of choice.
- Defenders must protect systems at all hours of the day and night, whereas an attacker can attack at a time of his or her choosing.
- Defenders must conform to policies and obey all applicable laws, whereas an attacker can break any law at any time.

Organizations Hiring InfoSec Professionals

These days it might be easier to ask, what types of organizations *don't* hire information security professionals? Every organization that uses computers and networks must employ people with security skills and knowledge. With the frequency of malware attacks, even a one-person IT department must be knowledgeable about basic security skills.

The following types of technology activities beg for security skills:

- Providing secure Internet connections
- Managing login credentials and access known as Identity Access Management
- Allowing secure remote access for valid users
- Providing supplier, partner, or customer access via Virtual Private Networks
- Maintaining secure email servers
- Managing and protecting the information on file servers
- Managing laptop computers for a mobile workforce

- Creating secure in-house written software
- Maintaining enterprise application access with user accounts

When an organization has one or more of the preceding in its technology environment, the organization's IT department had better have one or more of its IT people with some security skills. Otherwise, a lot is going to go wrong. I present the preceding list again, only this time I've added the consequences of poor security:

- **Internet connection:** Attacks from the Internet; malware from watering hole attacks.
- **Login credentials:** Attackers who stop at nothing to guess login credentials, including the use of automated tools that can perform brute-force attacks, in which thousands of different passwords per hour are guessed until the right one is found. Then it's "game over"!
- **Remote access:** Brute-force attacks against user accounts, eventually leading to successful break-ins.
- **Supplier, partner, or customer access:** Attacks from supplier, partner, or customer organizations. Misuse and abuse by personnel with poor judgment in those organizations.
- **Email server:** Incoming spam, malware, and phishing attacks.
- **File server:** Access management issues, data loss through lax access permissions; malware hosted on file server.
- **Laptop computers:** Stolen laptop computers with loss of data stored on them; attempts to break into organizations based on login information stored on stolen laptops.
- **In-house written software:** Exploitable vulnerabilities leading to data loss.
- **Enterprise applications:** Access management issues, people with excessive access privileges, terminated employees with still-active user accounts.

Now, look at the list one last time, to see what technology and security professionals need to do to protect systems and data:

- **Internet connection:** Network engineers need to understand how to make *edge devices* (the routers, firewalls, and other devices at an organization's outer boundary) resistant to attack. They also need to be able to install and manage firewalls and other protective devices with their complex rulesets to let the good guys in and keep the bad guys out, and to prevent malicious software from getting into the organization.

- **Login credentials:** User IDs, passwords, and security tokens are issued only to authorized personnel. In larger organizations, automated tools are used to reduce errors and watch for problems. Many systems can be configured to prevent brute-force attacks.
- **Remote access:** Some personnel must have access to an organization's internal network from any location. A remote access system must be built correctly so that only authorized personnel can get in.
- **Supplier, partner, or customer access:** Most organizations rely on other organizations for supplies, personnel, or services. In many such cases, people in those external organizations need access to internal resources. Every aspect of this process must be done right to prevent cybercriminals from exploiting external access and stealing data.
- **Email server:** Because email servers are connected to the Internet, systems engineers need to know how to correctly configure and "harden" email servers to prevent intruders from compromising the organization's email communications.
- **File server:** Internal and external file servers must be correctly configured and managed to protect all sensitive information stored on them and to prevent intruders from being able to access sensitive data.
- **Laptop computers:** Personnel who build and manage laptop computers (as well as tablets and other cool devices that we all want) must include the latest measures, such as whole-disk encryption and advanced malware prevention tools, to prevent the compromise of data stolen on laptops, as well as to protect the systems that laptops are permitted to connect to.
- **In-house written software:** Software developers need to understand how to write software that will be resistant to attacks such as buffer overflow, script injection, and authentication bypass.
- **Enterprise application with user accounts:** Personnel who manage user accounts for enterprise applications need to keep accurate records and use detailed procedures to make sure that no unauthorized personnel are given user accounts. Also, applications must be configured to track all user logins, and create alerts if any user accounts are under attack.

As you can see from this list, which is but a sampling of all the aspects that require security expertise in an organization, a wide set of skills is required for all IT workers, including specialized security personnel.

Chapter 2

Understanding InfoSec Roles: One Day in the Life

In This Chapter

- Understanding the paths to achieving a security job
- Exploring the array of security-related jobs
- Climbing to the heights of security management jobs

What is it like to have a security job?

Many people obtain security jobs after they've been in IT for a number of years. In many cases, the ability to get a security job is a matter of opportunity — being in the right place at the right time. However, a lot more than good luck is required; you need the desire and the aptitude for a security job.

Most people accumulated IT job experience and then move laterally into a security job. Others get a degree in computer science, management information systems, or information security and then get an entry-level InfoSec position. This chapter describes both job-hunting methods and also details the most common security jobs, from security analyst to CISO.

Getting Security Experience Where You Are Now

Workers early in their careers have the following complaint:

> *I want to get this new job, but it requires experience. How can I get experience if I don't have this job?*

Sounds like a chicken-or-egg problem, right? Not necessarily. Most security professionals didn't have a non-security-related job one day and a security job the next. Instead, they gained and built upon security skills in their current IT job.

In this section, you explore the following IT roles and discover how to build your information security knowledge and skills while in those roles:

- Service desk analyst
- Network administrator
- Systems administrator
- Database administrator
- Software developer
- Project manager
- Business analyst
- IT manager
- Human resources employee

All IT positions contain security-related skills and responsibilities. Everyone in IT should be aware of the security-related aspects of their jobs. IT workers are entrusted with a high level of privilege: they have access to sensitive data and the systems that control it.

Service desk analyst

A *service desk analyst* assists users how have problems with their computers, user accounts, or business applications. In some companies this position is the equivalent of a help desk technician or a PC fix-it dude (or dudette).

In many ways, service desk analysts have one of the most important non-security positions because they are in contact with users in all levels of the organization. For many employees, service desk analysts are the only IT people they will ever contact.

A service desk person must be able to recognize several types of security issues, such as the following:

- Forgotten passwords
- Requests to install software