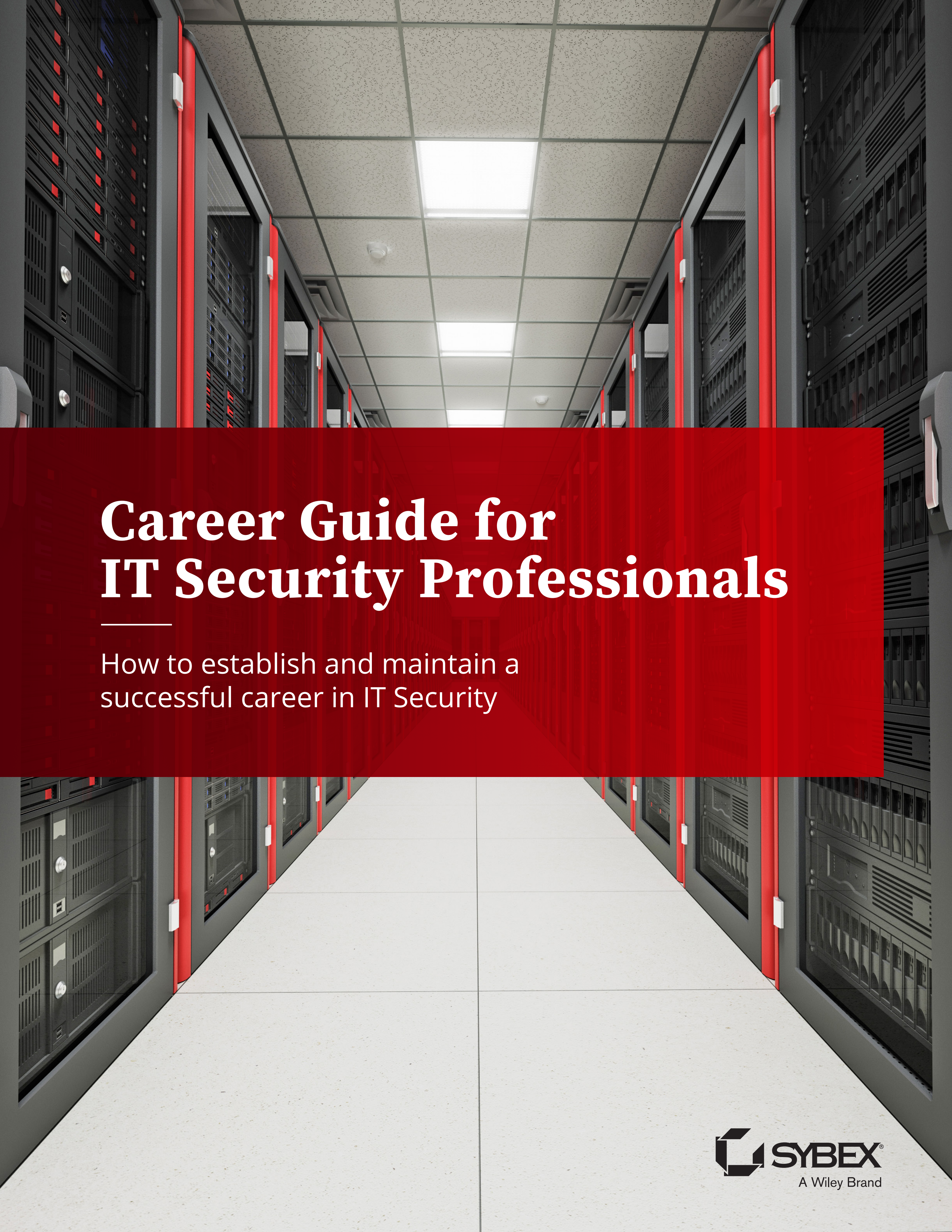

Career Guide for IT Security Professionals

How to establish and maintain a successful career in IT Security

SYBEX®
A Wiley Brand

© g-stockstudio/Getty Images

According to a report by idtheft.org, between 2005 and 2018 there were nearly 9,000 industry information breaches, exposing 1.07 billion records, and with the ability of hackers to continue to adjust to security measures, data is both more protected than ever.

Workers who have the ability to provide threat detection and employ security measures that enable them to provide IT security have a premium skillset. These days, companies know that data security is vital to a healthy operation, and a business without a strong cybersecurity backbone is a company that won't last long.

Cybersecurity personnel are responsible for the planning, implementation, upgrading, and monitoring of security measures that protect computer networks and information from intrusions by malicious or criminal means.

Secure networks are vital to the success of virtually every organization, so most medium-sized to large organizations have some cybersecurity personnel included in their org charts, if not an entire department devoted to securing data. In a smaller business environment, this position may be rolled into another IT position, but larger companies may employ a team of security professionals.

According to the Bureau of Labor Statistics, an Information Security Analyst has a median income of about $95,000 annually. With a job outlook predicting 28% growth between 2016 and 2026 (more than 4 times the average of all jobs), information security is a field any IT pro should be looking into.

Who’s Hiring You?

To be brief, virtually anyone who has any sensitive data housed in a network and/or computer system—be it customer or medical records, financial statements, or any other proprietary or classified information—has a need for digital security. This means just about every large business, corporation, or organization.

The level of security needed can vary widely, but whether it’s protecting customer credit card and banking information or protecting classified material at the government level, data needs to be secure and diligently protected from intrusions. Due to the nature of the job, cybersecurity requires a high level of trust among those working in it; in many cases, it literally requires high-level security clearances.

Speaking of the government, protecting a country’s sensitive data is more important than ever in the digital age, and the government is one of the top employers of IT security personnel. These jobs are often rather lucrative to those who hold them but are often difficult to get since the security clearances are so complicated.

Entry Level

Since the IT industry is still relatively young, cybersecurity is still a burgeoning career path and has a less-defined structure than many established careers. The onboarding track for security professionals is somewhat loosely defined, and many employers are simply not certain about what an industry-standard cybersecurity pro looks like.

Many of today’s industry leaders say practical job experience and certifications are key to getting a foot in the IT security career door. In many cases, it’s equally as important as, or equivalent to, a two- or four-year degree, which has been the preferred path. However, many companies are now offering their own certifications—in addition to still requiring a mastery of hardware and software, problem solving abilities, and good communication.

Getting Started

Whether you choose to pursue a traditional degree or take the trade school or certifications route, education is a vital component of IT security. It’s a quickly evolving profession, and the information you have today may soon be outdated. Staying diligent and keeping abreast of trends is critical, but for those looking at the bigger picture (and for a middle- or upper-management position), earning a traditional degree is still a sound strategy.

You can find a pathway into the core cybersecurity jobs by using more common IT roles like networking, software development, systems engineering, security intelligence, and financial and risk analysis. These will help you develop a working fluency and a knowledge of firewalls, Linux, Python, UNIX, TCP/IP, and Cisco systems.

Core competencies such as these will help ensure you are prepared to get into the high-stakes game of cybersecurity, but don't skimp on the so-called "soft skills." IT Security involves a great deal of complex problem-solving skills, critical thinking, communication, and active listening skills.

It is also important to keep in mind that the IT Security field is a "destination" job; you aren't likely to simply fall into one without a little experience under your belt. Many cybersecurity pros started in "feeder" positions like networking or helpdesk IT-type roles before transitioning into cybersecurity after they gained some experience. Once you've gained experience in these types of roles, you can target entry-level cybersecurity jobs.

Entry-Level Job Titles

Security Analyst

Threat Analyst

Cyber Security Analyst

IT Security Analyst

Cyber Crime Investigator/Analyst

IT Auditor

Cyber Intelligence Analyst

If these jobs evoke images of police work, you're not far off base. There is a great deal of investigative work done in many of these roles. Problem solving and deductive reasoning are important skills for the job, and many organizations even use police-type job titles, including "detective," "investigator," or "officer" for certain positions.

Your role will largely entail targeting and eliminating threats and vulnerabilities in your organization's IT infrastructure. At this early stage of your career, you'll be taking orders from management, implementing the company's cybersecurity strategy, and closing individual vulnerabilities.

These positions pay commensurately, too; they carry an average salary that ranges from about $70,000 to $88,000 annually. If that seems like a lot for an "entry-level" position, keep in mind that 1) you will likely have to be in the industry for a few years in different positions as you grow into the role, and 2) you'll earn your keep when you get there. You will toil for a while in lower-paying jobs with less responsibility like helpdesk and end-user support.

You'll be expected to have a working knowledge of Linux, as well as some project management, security operations, system administration, and network security abilities. So while cybersecurity is an in-demand career path, it also typically takes a couple of extra years to land those "entry-level" positions.

Education/Certifications

Certifications are among the most powerful allies you can have in an IT security career. For employers, they act as a sort of shorthand for gauging both the level of your skills and the seriousness with which you take your work. Some entry-level workers may try to lean on their raw talent more than taking the time (and expense) to provide a quantifiable means to measure how well they are able to do their job. It's simple: it doesn't matter how good you are at your job if you can't prove it. Certifications validate your skills.

Additionally, many employers will often foot the bill to get their employees certified, giving them free rein to build professional skills ostensibly *for free*. If you aren't taking advantage of a deal like that, you are missing out on a golden opportunity, and you do so at your own peril.

Here are a few of the certifications you should be looking at taking (or should already have completed) as you start the early stages of your career:

CompTIA Security+

CompTIA A+

CompTIA IT Fundamentals

Moving Forward

Once you get into the cybersecurity game, you might think you're in, but remember, you're only at the ground level. If you want to get to the penthouse, you still have plenty of work to do. Here are a few tips for how to advance into the next phase (and salary structure) of the IT security field.

Be a team player. No matter what the role, companies are looking for leaders. If you're someone who works well with others, you most likely have the respect and/or admiration of the department. Reach out to others to help them when they need it, and don't be afraid to ask for help yourself. Remember that collaboration is key in learning and in gaining experience, two vital parts of becoming a stronger professional.

Be the volunteer. The "go-to" guy or gal is the one who gets the most attention. Don't shy away from tackling those issues no one wants to take on. There is no better way to gain experience than to volunteer to take on the problem cases. Your skills will increase, and you will look like a leader to your peers and to your supervisors alike.

Certs, certs, certs. Have the latest certifications, and stay on top of the newest trends. New vulnerabilities crop up all the time, and if you can identify and close them, you'll be a hero to the higher-ups. IT security isn't a field where you can grab your degree and settle into your job. You need to be proactive with pursuing the newest, most updated certifications and never stop learning.

Build your skills and experience. Every bit as much as certifications, real work experience is as important as any single factor both in securing new employment and in advancing. It's great to have a passing familiarity with every aspect of the job, but you should focus on one or two areas that you really specialize in.

Understand the critical role people and processes make in keeping out threats. Technology has made great advancements in locking down critical systems, but always remember that a firewall or intrusion detection system can't fix every problem. There is nothing like the experiences of a skilled employee to sniff out a potential issue before it becomes a major problem.

Mid Level

As you gain experience in the cybersecurity field, you should find success coming your way. By the time you've had 5-7 years in the industry, you should be beginning to reach the middle portion of your career. No longer are you a noob; you're in the game and have the experience to take the lead when necessary in certain situations. With the knowledge you have built over the past several years comes trust; your managers know that you can be relied on in a pinch.

At this level, you are expected to be able to identify threat mitigation techniques and remain up to date on the latest strategies and programs to combat these methods as they continue to evolve.

Getting Started

There is a dearth of solid mid-level talent in IT Security today, so the next 10-15 years will have a great deal of opportunity as today's entry-level cybersecurity staff will be tomorrow's middle management. Much of today's top talent has migrated to the executive level—where they are busy conceptualizing new strategies to prevent data breaches or responding to seal off vulnerabilities—leaving openings in the middle that need to be filled.

That means you need to build a large information security skill base—now. Do you have solid Linux and UNIX skills? Continue to develop your knowledge of information systems, cryptography, and network security. More than a passing familiarity, you should have intermediate to advanced user skills in these areas, continuing to develop them even amidst frequent changes in process, interface, and technique. This is the time to learn some new tricks, gain a working knowledge in a new area or two, and continue to build on the skills you already have. Be sure you're always plumping up that skills toolbox.

As you reach this level, you might be surprised to learn that your "soft skills" will start coming more into play. You will still largely be working to implement your company's IT strategies, but you will begin seeing the bigger picture—and your conversations with management may be evolving, with more talk of conceptual issues than simply implementing what is already there. Your project management, business process, risk management, and problem-solving skills will all be tested, and if you want to be able to rise in the ranks, expect to have (or develop) solid people skills. Focus on sharpening those communication skills; seminars, conferences, and even continuing education classes are a good place to start. They'll start serving you soon enough, if they haven't already.

Mid-Level Job Titles

Cybersecurity Analyst

Cybersecurity Consultant

Penetration & Vulnerability Tester

Senior Security Consultant

IT Security Consultant

Is this a lot of work? Most definitely, but the rewards are bountiful. A Penetration and Vulnerability Tester can expect to command a salary in the high $90,000's, while a Cybersecurity Consultant/ Manager or Engineer crosses six figures with salaries averaging up to $107,000. The stakes, though, are as high as the salary, and these jobs carry a great deal of responsibility—and quite often there is a great deal of job pressure. After all, the cybersecurity worker is tasked with protecting some of the most sensitive information in people's lives.

Education/Certifications

These certifications will help bring you into a new career bracket. With their more advanced focuses on protection strategies, tools, and abilities, you'll find you're able to step up your game accordingly.

CompTIA CyberSecurity Analyst+ (CySA+)

CompTIA Network+

CompTIA Server+

Certified Ethical Hacker (CEH)

Microsoft Certified Solutions Associate (MCSA)

GIAC Certified Incident Handler (GCIH)

GIAC Security Essentials Certification

Citrix Certified Integration Architect (CCIA)

Again, pursue as many of these as your bosses deem necessary, and continue to grow your skillsets. By this time, you should be moving away from one-size-fits-all solutions and should be delving into one or two specific areas of security. Become an expert in something rather than a novice in everything.

Moving Forward

It's at this level that a solid secondary education begins to make the difference. You may be creeping into middle management roles, so employers want to see those degrees. At the very least, you'll be forced to really prove yourself through experience and certifications if you are lacking at least a bachelor's degree. Cyberseek.org says 73% of the employees in a middle management role hold a bachelor's degree, and an additional 15% hold a graduate degree. In other words, if you have designs on advancing further in a cybersecurity career, you almost certainly need a bachelor's, and you might want to start thinking about a master's degree, especially if you want to reach the executive level.

Senior Level

When you’ve been in the business long enough to reach the senior level, you should be looking to the pinnacle of your career. Your years, most likely counting in decades by now, have given you experiences that have you looking at security breaches and intrusions conceptually more than reactively, and if you’ve played your cards right, you’re either in upper middle management or perhaps even peeking up at the executive level.

Getting Started

Your promotion or acceptance of a senior-level position marks the beginning of this phase of your career. In general, at this stage, you assume a higher level of responsibility for the safety and integrity of your organization’s data.

As with many IT management jobs, while it’s important to be aware of the latest methods in cybercrime prevention, you likely won’t be taking as active a role in performing some of the physical tasks. You may not be putting your hands on the tools to stave off a security breach, but you are leading the way in implementing the protections, guiding and training your staff, and managing security audits and threat assessments.

You’re likely to focus on company-wide initiatives, developing policies, and ensuring those working under you have the proper training, skills, and certifications to perform their jobs at a high level.

Education/Certifications

You might be a veteran, but the timeworn adage about teaching an old dog new tricks is a myth. In the world of cybersecurity, it had better be. Continue building your skills, developing new processes and abilities, and forging ahead into higher and higher levels.

By this stage, though, your skills might begin creeping back away from specifics and back into a more general stage. When you’re in management, you’re looking at building concepts and then putting staff in place to make those concepts reality.

Senior Level Job Titles

- Cybersecurity Manager
- Cybersecurity Administrator
- Information Systems Security Manager
- Cybersecurity Architect
- Cybersecurity Engineer
- Chief Information Security Officer
- Threat Intelligence and Security
- Operations Center Professional
- Chief Information Security Officer
- Chief Security Officer
- Digital Forensics Officer

Many of these jobs are made up largely of advanced, specialized, high-level threat detection roles or are either executive-level or upper-mid management spots designed for people who think broadly about risk and who have the technology skills and communications abilities to understand and explain technical concepts in business terms to an organization's board or audit committee. In other words, you have to provide and implement broad, organizational-level plans for risk management and put those plans into terms that your board of directors, executives, or other bosses will understand.

Remember those non-technical "soft skills" you were working on during the middle portion of your career? They are coming to the forefront now. Working with and motivating your staff to implement your policies and procedures is now a significant part of your job. Problem solving and communication are common competencies for cybersecurity veterans and are essential to the daily completion of your job.

While senior positions require a great deal of experience, skills, and certifications, you are commanding a significantly higher salary than in lower-level jobs. Depending on the position, the company, and the skills required, you can expect to be earning mid to high six figures working in cybersecurity. An Information Systems Security Manager, for example, can earn upwards of $200,000 annually (according to Robert Half's® international 2018 Technology and IT Salary Guide).

Cisco Certified Network Professional (CCNP)

Cloud Security Certificate of Cloud Security Knowledge (CCSK)

Cisco Certified Design Professional (CCDP)

CompTIA Advanced Security Practitioner (CASP)

Cisco Certified Internetwork Expert (CCIE)

Certified Information Security Manager (CISM)

Certified Information Systems Security Professional (CISSP)

Security Cisco Networks with Threat Detection and Analysis (SCYBER)

Summing It All Up

All levels of IT security professionals are in high demand. With thousands of additional jobs available and large growth prospects, it's a great field to get into on the ground floor. Yes, you're going to work for your money, but the rewards of a job well done are many in this field. And for those with a passion for cybersecurity and a knack for preventing intrusions, eliminating threats, and patching vulnerabilities, you'll have a continually evolving career track paved with opportunities for success.

For more information on how to establish and maintain a successful career in IT Security, visit **www.wiley.com/learn/professionaltech/.**

Cover photo © i3d/Shutterstock

SYBEX®
A Wiley Brand