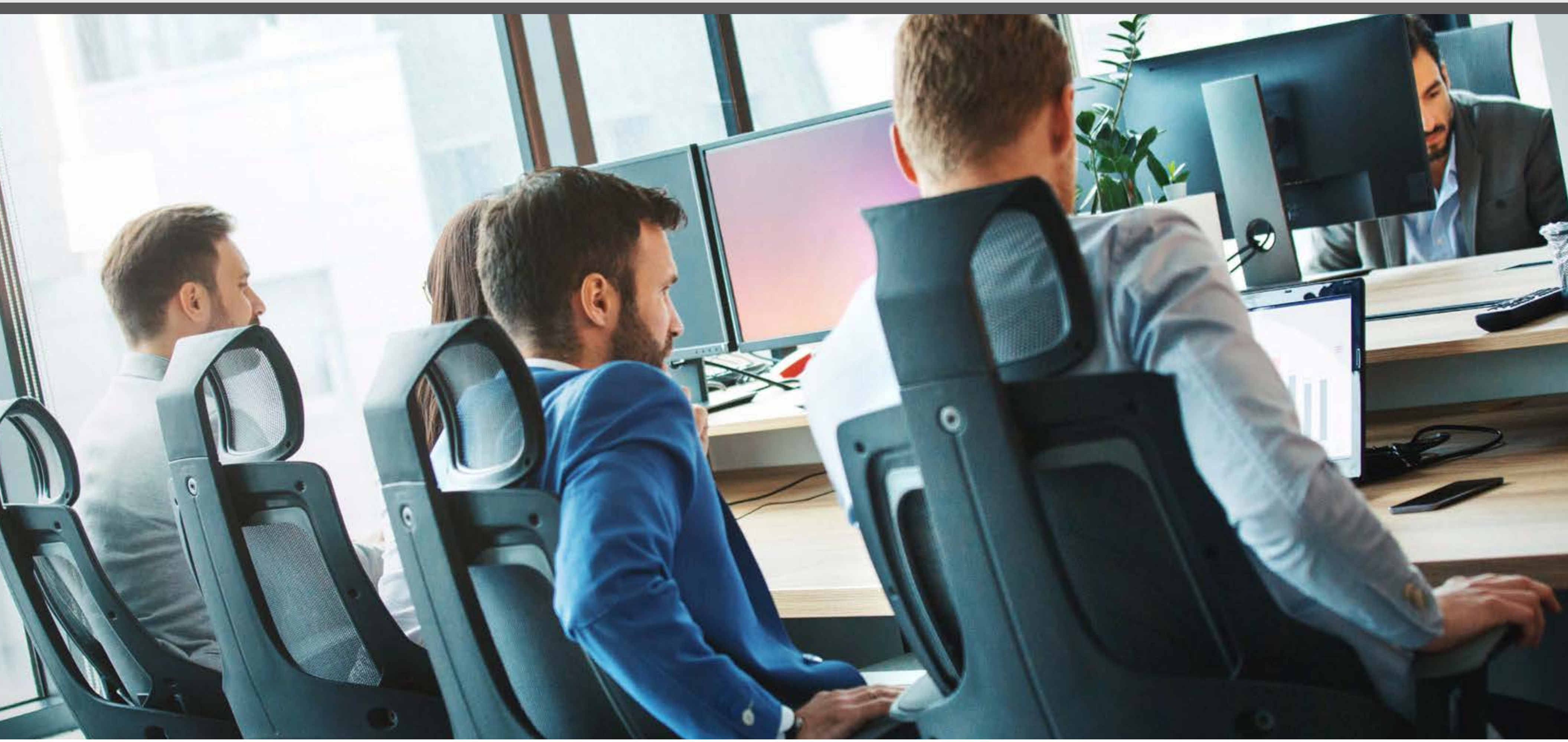
CYBERSECURITY CAREER GUIDE:

Advancing Your Career at Any Stage



CAREERS IN CYBERSECURITY

Table of Contents

Introduction: Cybersecurity Offers Limitless Career Growth

The cybersecurity field continues to grow rapidly, and the need for experts is increasing within virtually every industry. In fact, the sector cannot fill jobs fast enough. According to CSO, which provides news, analysis and research on security and risk management, 1 million cybersecurity jobs are likely to remain open in 2017, and that number is expected to grow.

This shortage affords **countless opportunities** to those who want to further their cybersecurity careers. The nearly limitless number of possible career paths is exciting, but can also present challenges in knowing how to move forward. Education, skills and attitude are all key — but exactly what's needed differs with each career stage.

"Cybersecurity Career Guide: Advancing Your Career at Any Stage" offers insider advice from seasoned professionals for how to progress, whether you're an early-, middle- or senior-stage career insider. The guide features tips and inside knowledge from several experts, including these cybersecurity heavy hitters:

Our Experts:

Scott Schober

Cybersecurity author and communications CEO

- Award-winning inventor of cell phone detection devices
- Knowledgeable speaker on topics ranging from the latest threats in ransomware to technological solutions for distracted driving
- Author of "Hacked Again," an account of how even cybersecurity experts are susceptible to cyber intrusion

> "It's important to understand the hacker's mind and think about their motive. It's not always money. Sometimes it's the challenge of doing something you're not supposed to do."

Daniel Miessler

Information security executive and blogger

- Former U.S. Army intelligence analyst
- Active content developer with more than 2,500 essays, posts, tutorials, articles and podcasts available at https://danielmiessler.com
- Director, client advisory services for security consultancy IOActive, Inc.

> "Find things you care about and help make them better. Don't chase the credit; make it about the output and the credit will come."

Eric Vanderburg

Security investigator and author/speaker

- Continual learner with more than 40 technology and security certifications
- Regular presenter and author of several books and the Security Thinking Cap blog
- Social media channels often cited as must-read content for technology and security professionals

> "A person in cybersecurity should demonstrate that they are a continual learner by striving to stay ahead of the technology curve — and never stop reading."

CYBERSECURITY CAREER GUIDE:

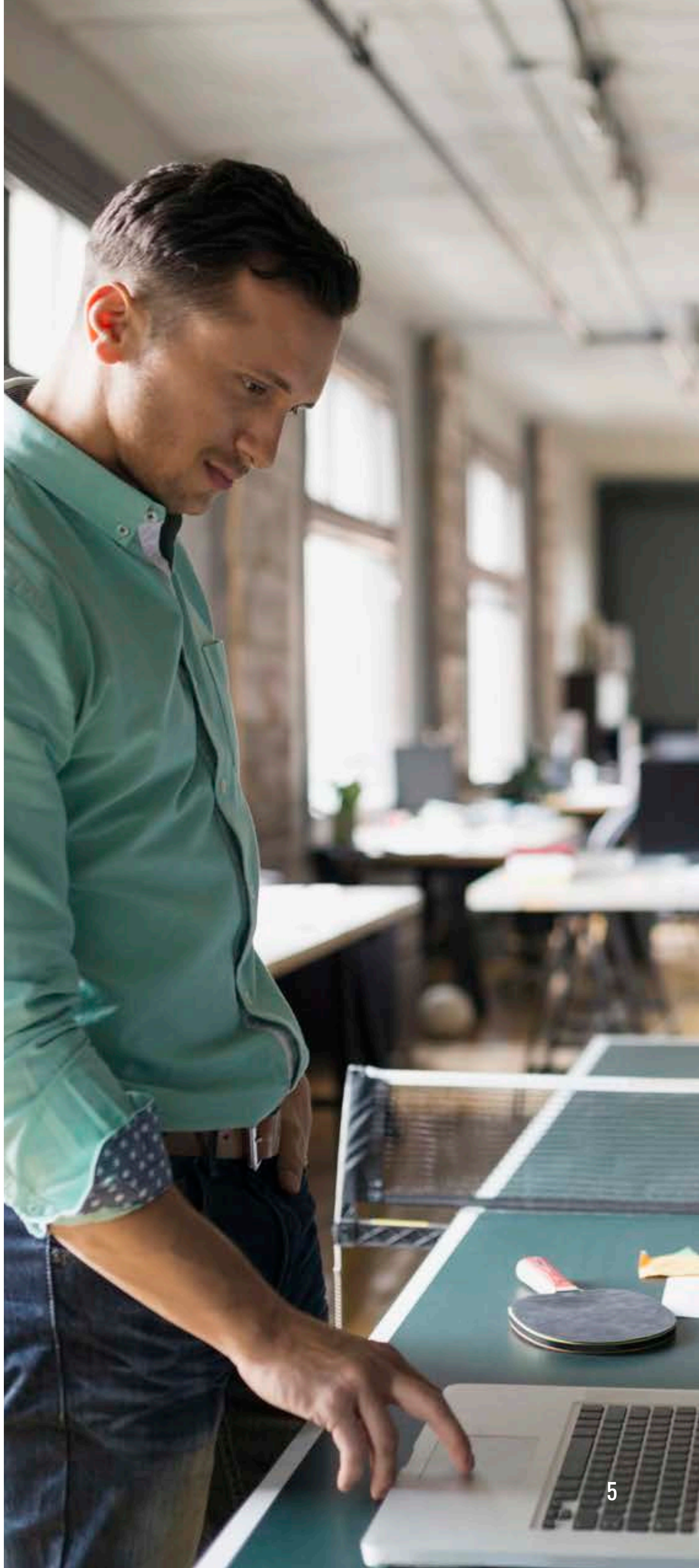
Advancing Your Career at Any Stage

Like the process of combating cyber threats, the path to career success within the cybersecurity field isn't always obvious, even to those who have been working in it for years. As in any field, the best advice comes from those who have been there, and the following pages include key strategies from a few of the leading cybersecurity professionals:

- We start with a look at education, certifications and other actions needed to get beyond the entry-level stage. In particular, we'll explore why passion is so important at this stage.
- Then we examine how cybersecurity professionals can gain additional skills, and take the next step into mid-level management.
- Finally, we'll look at the late or executive stage, and discover how landing a top job doesn't mean it's time to relax.

In addition, throughout, we've included spotlights on critical skills, such as the importance of passion, networking, tips for managers new to cybersecurity and the best cybersecurity resources.

The experts quoted here — as well as other trusted sources — offer actionable suggestions that, when followed, will lead to a long and fulfilling cybersecurity career.



Section 1: Early Career

BEYOND ENTRY LEVEL

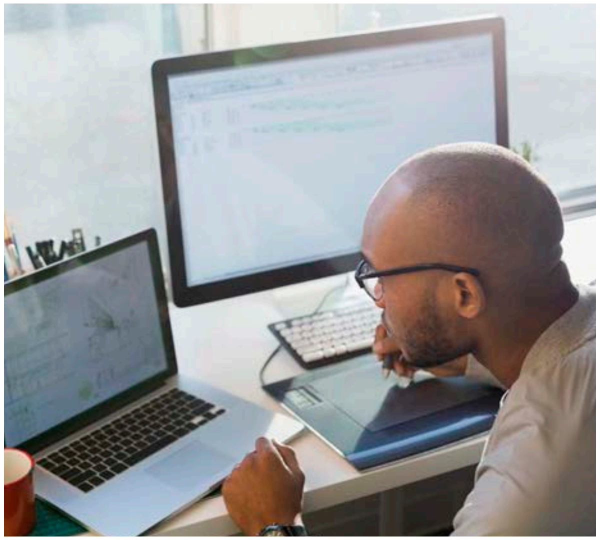
Those in the early-career stage should start by mapping out where they'd like their career to lead. Job seekers should consider criteria such as pay, location, hours, level of challenge and opportunities for advancement. Once you've identified a particular position, you can determine interim steps. For example, those interested in targeting a chief information security officer (CISO) role can get on the right track by pursuing a systems security position and learning managerial skills.

In addition, look at preferred job descriptions to see which degrees and certifications are most commonly required in your chosen roles. Advanced degrees are becoming a more common requirement for certain positions, including CISO.

Those interested in joining the sector from another field may need to get additional training. Daniel Miessler is an information security practitioner and blogger. As director of advisory services at IOActive, he recommends that anyone getting into cybersecurity should have a background in system administration, networking or development.

Kelly Sheridan is associate editor at Dark Reading, and has written dozens of business IT articles for InformationWeek. She notes that certifications are also "valuable in securing an InfoSec job." She states, "The certification you choose depends on your skills, background and desired position."

Because there are so many educational alternatives — including part-time, accelerated and online programs — it's important to be aware of the many emerging trends and options available.



TOP TIPS:

Building a Cybersecurity Career

GET EDUCATED:

Experts recommend a degree in cybersecurity, system administration, networking or development.

ADD CERTIFICATIONS:

Courses in specific skills provide a niche focus.

BUILD A NETWORK:

Get to know others in the field. Attend meetings and start trading techniques and resources.

SEEK A MENTOR:

Build relationships, until you find someone who has been in the field longer than you and who is willing to provide valuable insider tips and advice you won't find anywhere else.

SHOW ENTHUSIASM:

After a few months in your first job, do a self-check to make sure you still have passion for the work. Those who don't love the field are less likely to thrive in it.

LEARN FROM THE BEST

Those who want to stand out in cybersecurity should also take advantage of a less obvious type of education: mentoring. A good mentor in your chosen niche can share how they handled challenges you may be facing, or guide you toward smart career moves.

Finding the right mentor may take some time, but it will be well worth it. Your current company is a good place to start: Build relationships by being a team player and volunteering for extra responsibility. As you enhance your visibility, ask a more experienced professional who you admire if they would like to engage with you in this way.

Or, seek potential candidates out at professional organization meetings or conferences. Eric Vanderburg has been working as an innovator and business leader for over 15 years, and regularly presents at seminars and colleges, and publishes IT and business-related magazine articles. He currently serves as director, information systems and security at Jurinnov, a cybersecurity, forensics and legal consulting company. He suggests, "[Don't] wait till you are in your middle career to do it. I found a mentor shortly after starting in the industry and have mentored those who haven't even entered the industry yet. There is hardly ever a time when the experience of someone who has gone before you cannot be put to good use."

Know in advance what kinds of topics or decisions you'd like help with, and propose a mutually agreeable meeting schedule.

THE IMPORTANCE OF PROFESSIONAL PASSION

Perhaps more important than any other element in a cybersecurity career is passion.

Consider penetration testers (i.e. "ethical hackers" or "white-hat hackers"), who use their skills to predict how cybercriminals might attempt to crack open databanks, and share their results with colleagues who can strengthen those systems. Similar to their malicious counterparts, these testers experience the excitement of pushing boundaries.

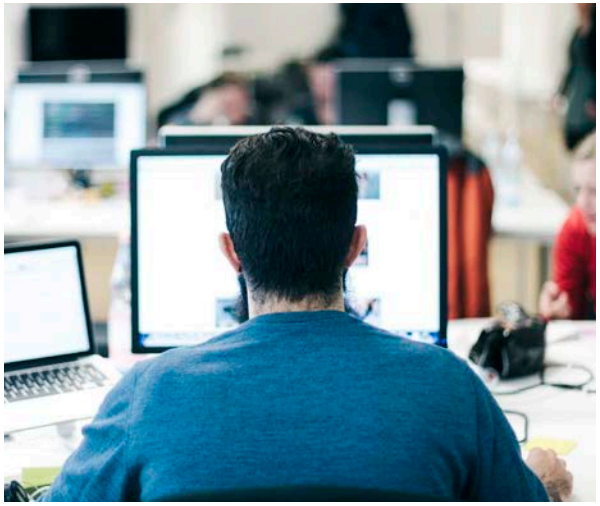
Cybersecurity blogger Daniel Miessler comments,

> "Most who stay with infosec for many years, and who are successful, achieve success because they're ... up late at night writing a tool or a blog post not because it's the scheduled time, but because they're physically unable to do otherwise."

FOCUS, FOCUS, FOCUS

In the early part of your cybersecurity career, it's important to choose a focus area. It may be that you've already chosen one, but if not, the time is now. Choosing a niche sector will help you narrow your career choices, and define the degree and certification options you pursue.

Cybersecurity expert Scott Schober suggests, "Home in on and industry where you can fine-tune. It could be retail – helping to protect financial data – or education; there's a huge need for educators within the CS field. Transportation is an exploding area as well. These are just a few examples of niches within cybersecurity, each one requiring a different career approach."



SHAUN KELLEY

Forensic Technology Associate

After earning a bachelor's degree in criminology and computer applications, Shaun Kelley followed it with a master's degree in cybersecurity and computer forensics from Utica College. While earning his degrees, he interned at the Computers Department of State University of New York (SUNY) and with the Cortland County District Attorney's Office. These positions prepared him for his first professional position as a forensic technology associate at KPMG, where he provides forensic services to Fortune 500 companies.

> *I was able to get a job in the field from the networking I did as a student. Since joining KPMG, I have been able to use the skills I have developed in this program (both technical and social) to solve real-world problems in the workplace.*

DON'T WAIT TO BUILD YOUR NETWORK

Getting to know individuals in your field is critical, and it's never too soon to start. Networking can help you get a job, explore your chosen niche or learn new skills.

Growing up, cybersecurity speaker, author and inventor Scott Schober was a gamer and belonged to a computer club. His dad worked at Atari, so he's been entrenched in IT his entire life. Now the CEO of Berkeley Varitronics Systems and author of "Hacked Again," he regularly speaks about working in the cybersecurity sector. "If you want to learn fast, surround yourself with people who are smarter than you," he says. "Connect with peers, share techniques and learn from others."

Remember that networking isn't limited to attending professional organization meetings, and that it's an ongoing process. The person you meet today at your kid's soccer game could be in a position to offer you a job, or direct you to someone else who can, a year down the road.

Section 2: Middle Management

KEY MOVES FOR CLIMBING THE LADDER

When considering going for a management position, it's critical to understand a cybersecurity manager's typical responsibilities. They include monitoring operations and infrastructure, ensuring regulation compliance, auditing policies and controls, and developing a security incident response program.

To prepare for these responsibilities, you may need to gain additional skills — often the kind you can't get a certification in. Success depends on understanding the business, being able to communicate with all departments within the business, and getting noticed in positive ways.

Lorna Koppel has built an impressive career in IT and infosec over the last 20 years, and is currently director of information security for Tufts University. She explains: "Your No. 1 role is to enable the business ... The first thing is accepting that you have to work on your business acumen and your communication skill sets and understanding what's important to the business." Specifically, Koppel recommends professionals look at key projects and strategic plans within the business to understand how it makes a profit and what its priorities are.

IN IT TOGETHER

According to speaker and author Scott Schober, another key to moving into management is being prepared to communicate outside of your department. "Cybersecurity goes beyond IT to areas like HR," he says. "You have to be willing to cross bridges and get along with all departments to maintain company policy. Cybersecurity is everyone's problem and everyone's solution, so a lot of it is about communicating best practices to all areas of the business."

Much of this communication will be related to intentional and unintentional internal threats. According to the Harvard Business Review, cybersecurity managers must have the skills to identify the company's most valuable information, and protect it using data, analytics and strong security standards. Such skills can be built through working closely with someone who already carries out these duties.

TOP TIPS:

Routes to Management

UNDERSTAND THE JOB:

Read up on responsibilities specific to management positions, like monitoring operations and developing a security incident response program.

LEARN ABOUT BUSINESS:

Observe the business side of the company and ask questions about how decisions are made.

POLISH SOFT SKILLS:

Consider courses in leadership, project management or communication.

WORK COLLABORATIVELY:

Think about how cybersecurity touches all corners of the company and identify ways to help to ensure compliance in every department.

RAISE YOUR PROFILE:

As much as possible, become more visible with extra projects, an online presence or speaking engagements.

EXPLORE HIGHER EDUCATION:

Consider getting a master's degree or other advanced education or certifications to show that you're committed for the long run.

GETTING NOTICED

> *It's not enough at this level to simply execute on what you've been given. You have to be able to innovate.*
>
> – Daniel Miessler

Learning new skills, getting additional education or certification, and seeing the big picture in terms of how cybersecurity affects all areas of the business may sound like a lot to take on — and it is! But there is yet another element that's critical for management, and that is serving as a public face for the company.

Cybersecurity executive Daniel Miessler explains, "It's not enough at this level to simply execute on what you've been given. You have to be able to innovate." He recommends some actions for getting noticed, including **lending expertise** to others' projects, maintaining an **online presence**, attending and speaking at **conferences** and earning a cybersecurity **master's degree**.

These actions make you more visible to potential managers within your company and within the industry, and mark you as someone who has made the extra effort to anticipate future cybersecurity threats and trends.

Explore cybersecurity master's degrees.

ERIC VANDERBURG

Director, Information Systems and Security, Jurinnov

After earning bachelor's and MBA degrees in technology at Kent State University, Eric Vanderburg went on to earn his doctorate in Information Assurance at the University of Fairfax. He now directs the cybersecurity consulting practice as well as the information technology team at Jurinnov, a cybersecurity, forensics and legal consulting company that specializes in helping companies recover after a data breach. He is also vice chairman of the board for Technology Ministry Network, a nonprofit organization that equips those in ministry with technology tools and training to accomplish their goals.

> *Goals are excellent, and you should set exciting stretch goals for yourself, but understand that each goal would not be accomplished if not for the successes of the moment. Recognize those successes and take the time to cherish and celebrate them.*

ARE YOU AN EXPERIENCED MANAGER, BUT NEW TO CYBERSECURITY?

For those considering a mid-career switch into cybersecurity, there are many pathways to leadership roles. Additional training paired with an advanced degree can blend with expertise earned elsewhere to create unique value within the field.

Presenter and executive Eric Vanderburg says, "Cybersecurity touches on many aspects of the organization, and your individual discipline and experience can give you insight into that part of cybersecurity. For example, those in HR would relate to employee training, onboarding and termination procedures, employee screening and background checks, and employee compliance requirements. A person from an accounting background could understand the SOC/SSAE accreditation process, ROI and the financial impact of implementing new systems."

A cybersecurity master's degree can be particularly useful when pursuing a management position, because it teaches skills that make applicants extremely qualified for top leadership positions. Plus, those with advanced degrees are paid better than those without. Additional certifications don't hurt, either.

Section 3: Senior Leadership

CYBERSECURITY CORNER OFFICES: ANYTHING BUT CUSHY

New cyber threats are constantly appearing, so top officers in this sector must stay abreast of current developments at all times. Unlike in other fields, where experienced leaders might be slowing their pace and thinking about retirement, cybersecurity executives must guard against complacency.

Cybersecurity speaker and author Scott Schober observes: "In cybersecurity, you never reach a pinnacle in your career. You can never be satisfied, but instead must keep working to stay ahead of the hackers."

> "If you're not staying current, then you've already lost."
>
> **– Matt Sarrel**

GIVING BACK

As a senior leader, part of your job is to help those in earlier stages of their careers. There are several ways you can do this, including acting as a mentor, speaking at conferences and addressing high-level challenges within the industry.

Seeking someone to mentor is similar to the process of seeking a mentor. First, evaluate what you have to offer, how much time you're willing to spend and what your specialties are. Then, start with colleagues within your company, keeping an eye out for young professionals who are highly motivated and learn quickly. You can also find potential candidates within professional organizations or at conferences. If your company or professional organization has a mentoring program, sign up for it.

To get more involved with speaking, maintain a calendar of relevant conferences and when submissions for speaking are due. Keep your résumé and press packet up-to-date, and announce on your website or other points of presence online that you're available to speak, and which topics you can cover.

TOP TIPS:

Staying Engaged as a Cybersecurity Executive

STAY INFORMED:

Make it a priority to seek out information about new threats.

BE CURIOUS:

Find news outlets, industry organizations and other sources to learn about innovations and new ways of doing things.

GET OUT THERE:

Attend and speak at conferences to share information and network with peers.

GET INVOLVED ON A HIGHER LEVEL:

Now is the time to lend your expertise through mentoring, speaking and addressing high-level challenges within the field.

CONSIDER A SWITCH:

A second career in a specialized niche might revitalize your dedication to the field.

Finally, seek out opportunities to improve the field for others who will come after you. Look back on your career and identify inequities, inefficiencies or other weaknesses that could be addressed.

> The thing that motivates me, more than anything else, is reducing the risk of harm to people potentially impacted by accidental or malicious data disasters.
>
> **– Sarah Clarke**

Devon Bryan is a former VP, global technical security services for ADP; he now serves as executive VP and CISO at the Federal Reserve. Throughout his long career he noticed the lack of diversity within the cybersecurity field. He explains, "Our future is hinged on technology. We need to change negative stereotypes and foster minorities' interest in this field early in their educational trajectory. For example, girls who may show an interest in STEM in elementary school can be deterred by perceptions that those careers are for men only. Why not require students to take technology courses, just as they have to learn a foreign language?"

KEEP IN TOUCH AND ON YOUR TOES

By the time you get to the late-career stage, you have most likely completed your schooling and certifications. But that doesn't mean you have finished your education. To remain informed as an industry leader, you have many resources to choose from. Technology journalist and technical marketing consultant Matt Sarrel recommends several online resources including:

- KREBS ON SECURITY
- INTERNET STORM CENTER
- STAYSAFEONLINE

In addition, there are many helpful lists (such as this one from Security Intelligence.com) that cover topics ranging from vulnerability of certain products to summaries of security incidents and organized cyberattacks.

Of course, as a senior career professional, you may be inspired to start your own blog, to build your own personal brand as a thought leader! There's nothing stopping you!

Conferences are also useful for learning about new developments and finding ways to diversify skills or fine-tune specialties. Popular events include:

- SHMOOCON
- BLACK HAT
- WOMEN IN CYBERSECURITY
- DEF CON
- INFOSEC WORLD

Bryan took action by founding the International Consortium of Minority Cybersecurity Professionals (ICMCP), a volunteer-run organization that creates a pipeline for diverse cybersecurity talent and career pathways for them once they've decided to enter the field.

CONSIDER A NEW DIRECTION

Another possibility for late-career cybersecurity professionals is to launch a second career or shift tracks. Sarah Clarke enjoyed a very successful IT and information security career for many years before shifting in 2016 into privacy and data protection, with a focus on making sense of the U.K.'s new General Data Protection Regulation (GDPR). This law aims to strengthen and unify data protection for individuals within the EU. "The thing that motivates me, more than anything else, is reducing the risk of harm to people potentially impacted by accidental or malicious data disasters," Clarke says.

Late-career professionals with a passion for a specific niche within cybersecurity may want to think about a similar move.

CISO may be one of the most important roles in the C-suite. Explore ways to get there.

DEVON BRYAN

Executive Vice President and Chief Information Security Officer

Devon Bryan's impressive career began with earning a bachelor's degree in applied mathematics and a master's in computer science. His first professional jobs were as an engineer and information security consultant. He held several positions within the Internal Revenue Service (IRS), as well as ADP, where he ended as vice president, global technical security services.

Following his VP role, Bryan moved to the Federal Reserve System where he serves as executive vice president and CISO. He is responsible for ensuring the information assets of the Federal Reserve Banks are well protected. He is also the founder and president of the International Consortium of Minority Cybersecurity Professionals (ICMCP), a volunteer-led organization that creates new career opportunities for under-represented populations.

> *As I talked with colleagues ... a common theme that surfaced in our conversations was not only the lack of talent in the market but lack of diverse talent. We decided that there had been enough dialogue about the problem, and it was time to DO something about it.*

A senior leadership position may sound like the end of a long career, but it may be just the beginning of rewarding mentoring relationships, speaking engagements, blogging, publishing – or an entirely new niche focus.

Conclusion

As a still-new field, cybersecurity holds great promise for those interested in contributing to the industry. New threats, emerging technologies and expansion of the need for this role within other fields all play a part in driving professional success. But, perhaps the strongest driver is each professional's curiosity. Those keen to enter and expand have excellent opportunities to pursue an exciting career and help build the industry.

Explore the cybersecurity career roadmap.