CYBERSECURITY
CAREER GUIDE

WHO WORKS IN CYBERSECURITY
HOW WE GOT STARTED
WHY WE NEED YOU

paloalto NETWORKS®

CYBERSECURITY CAREER GUIDE
Who Works in Cybersecurity? How We Got Started.
Why We Need You.

Publisher: Palo Alto Networks

Editor: Muoi Tran Landivar

Contributor: Elesa Cooperson

Copy Editor: Deirdre Beard

Design and Composition: Colleen Combes

Cybersecurity Career Guide: Who Works in Cybersecurity? How We Got Started. Why We Need You is published by: Palo Alto Networks, 3000 Tannery Way, Santa Clara, CA 95054, USA
Phone: +1 408-753-4000 | www.paloaltonetworks.com

First published: 2018

© September 2018

Cover Illustration by Tim Heraldo

Copyright in individual chapters rests with the authors. No photocopying: copyright licenses do not apply.

ISBN: 978-0-578-46393-3

Disclaimer

Cybersecurity Career Guide: Who Works in Cybersecurity? How We Got Started. Why We Need You. contains summary information about legal and regulatory aspects of cybersecurity governance and is current as of the date of its initial publication September 2018. Although the Guide may be revised and updated at some time in the future, the publishers and authors do not have a duty to update the information contained in the Guide, and will not be liable for any failure to update such information. The publishers and authors make no representation as to the completeness or accuracy of any information contained in the Guide.

This guide is written as a general guide only. It should not be relied upon as a substitute for specific professional advice. Professional advice should always be sought before taking any action based on the information provided. Every effort has been made to ensure that the information in this guide is correct at the time of publication. The views expressed in this guide are those of the authors. The publishers and authors do not accept responsibility for any errors or omissions contained herein. It is your responsibility to verify any information contained in the Guide before relying upon it.

Introduction: Let's Take a Look at the Numbers

Cybersecurity is a vast and dynamic field. To comprehend cybersecurity's steep growth and wide impact, let's take a look at a few numbers and what they mean.

- **Data:** First, we live in a digital age where humans and technology are bound together by a daunting amount of data. Ninety percent of all existing big data was generated in just the last two years, and we'll see 3,000 percent relative growth in the next two.[1] In other words, by 2020, there will be 44 zettabytes – that's 44,000 terabytes of data[2] – or 3,000 times the amount of data in Google® today. This data is worth a lot to the bad guys, and this is the data that cybersecurity practitioners work very hard to protect.

- **Humans:** The human attack surface is growing exponentially. By 2022, there will be six billion Internet users – that's 75 percent of the projected population of eight billion.[3] If not trained correctly, humans can be easy targets for attackers. On the other hand, if we are well-trained and have a strong culture of security, humans can be a very strong first line of defense.

- **Cost:** Cybersecurity breaches are more rampant than ever. By 2021, cybercrime damage costs will hit $6 trillion annually.[4] From 2017 to 2021, cyber spending will exceed $1 trillion.[5] It is estimated that ransomware damages would exceed $11.5 billion in 2019.[6] These are alarming numbers, and they are only a few indicators of how cybersecurity impacts every aspect of our lives. At work, at home, and in the community, we need the next generation of cybersecurity professionals to take action to protect ourselves and our information.

- **Workforce:** There will be 3.5 million unfilled cybersecurity jobs by 2021.[7] At a time when cybercriminals are becoming more sophisticated and adept, this is an important issue for all of us. Leaders in the cybersecurity industry are taking steps to help their organizations be better positioned to hire and train the next generation of security professionals. However, the need for more cybersecurity professionals is a challenge that will not go away on its own.

Cybersecurity needs you. We need your skills, experience, and problem-solving mindset to help solve for tomorrow's problems. You can be part of the digital ecosystem, where you have a unique opportunity to be thought leaders and shape the future of cybersecurity. **Will you join us?**

1. "What Is Big Data? Bringing big data to the enterprise," IBM, 2012, http://www-01.ibm.com/software/data/bigdata/.
2. "The Digital Universe of Opportunities," EMC Digital Universe with Research & Analysis by IDC, April 2014, https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm.
3. Steve Morgan, "2017 Official Annual Cybercrime Report," Cybersecurity Ventures, October 16, 2017, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.
4. Ibid.
5. Steve Morgan, "2018 Cybersecurity Market Report," Cybersecurity Ventures, May 31, 2017, https://cybersecurityventures.com/cybersecurity-market-report/.
6. Steve Morgan, "Ransomware Damage Report, Part 2," Cybersecurity Ventures, November 14, 2017, https://cybersecurityventures.com/ransomware-damage-report-2017-part-2/.
7. Steve Morgan, "Cybersecurity Jobs Report," Cybersecurity Ventures, May 31, 2017, https://cybersecurityventures.com/jobs/.

Table of Contents

Chapter 1:
Love Puzzles?
Enjoy Breaking Stuff?
Join Us!

Pamela Warren

Director of Government and Industry Initiatives
Palo Alto Networks

Years in Cybersecurity: 20+

"If you are interested in cybersecurity, the first thing I would recommend is to talk to people in as many different roles in security as possible. Cybersecurity is very broad."

A Day in the Life: I manage a team of security and networking practitioners from specific industries who share their expertise with our customers and prospects from their same industry. It's a unique opportunity within Marketing to have actual practitioners, including past customers, share their industry-specific security knowledge through webinars, white papers, blogs, roundtables and other channels. For example, our Financial Services security architect might create a secure IaaS use case for banking and then host a roundtable or give a webinar for financial services security practitioner peers who may be seeking guidance on that topic.

How I Got Started in Cybersecurity: I actually worked in a classified environment for the first 10 years of my career, and some of the projects that I got involved with during that time really piqued my interest in cybersecurity. At that time, it wasn't called "cybersecurity," but it was the importance of secure communications over any realm: telephone, Internet, and the like. I started learning more about cryptography, and it just really fascinated me. I knew I was hooked at that point. After my time in government, I was hired to work in a large semiconductor company in a new group that worked with security software vendors to take advantage of the newest chip capabilities. In this case, it happened to be a random number generator (RNG) in the chip set. This was before anyone knew what SSL was, and we needed to help users understand cryptography and the value of using an RNG to strengthen their encryption. It was an interesting job, and the more I learned, the more I wanted to do more in the field.

Take My Advice: If you are interested in cybersecurity, the first thing I would recommend is to talk to people in as many different roles in security as possible. Cybersecurity is very broad. There is the vendor side—with any role from Product Manager to Product Marketing Manager to Sales and Systems Engineering professionals. And there is the practitioners' side—from SOC threat analysts to DevOps Engineers. You could even get involved in media and report on cybersecurity. After having those conversations, you can make some educated decisions on a potential path that you'd like to pursue. Remember, nothing has to be permanent. You can always evolve your career as you learn more about your interests over time. It's not always about the destination: the career journey itself can be quite enlightening and the cybersecurity field is constantly evolving. I went from the

government to the semiconductor industry to my work at Palo Alto Networks, which is more interesting than I could have ever imagined. I didn't stick with one narrowly defined path, and as a result, the journey has been fascinating. I wouldn't want anybody to pigeonhole themselves and think, "If I go into product management, I have to always stay in product management." One of the things that I've learned is to always trust your intuition in every decision you make. We are all here with our unique gifts. Being able to trust our intuition on where to go and what to do next is really important. That has been a big part of my life and career. Let your passion—that's your intuition—be your guide.

Fun Fact: I was born with an innate and real passion for animals. I have been an active wildlife rehabilitator for over 25 years. Most recently, I've been working with harbor seals—from their rescue to rehabilitation to release—from day-old infants to adults, basically taking care of their needs until they can be released back into the ocean again.

Vidya Gopalakrishnan

Security Operations Engineer
Palo Alto Networks

Years in Cybersecurity: 2

"I've always been an avid crossword- and math-puzzle solver. During undergrad, I took a Cryptography and Network Security class. That naturally translated into me loving this course and getting interested in cybersecurity."

A Day in the Life: As a security operations engineer, I am responsible for defending the company's information and infrastructure against malicious threats. This involves activities such as incident response, working with IT teams to better harden the company's systems, and hunting for threats by leveraging information available from threat intelligence sources. As a security graduate student, I mainly specialized in Cyber Forensics and Incident Response Operations, which are more aligned with the defensive side of cybersecurity. I have learned how to deploy various tools in a SOC environment and how to effectively respond to threats. However, given the multi-disciplinary curriculum at my institute, I have developed a breadth of knowledge across disciplines, including ethical penetration testing, systems engineering, and engineering security-based systems such as malware engines, as well as other offbeat disciplines like deep-learning.

How I Got Started in Cybersecurity: In my junior year during undergrad, I took a cryptography and network security class. I've always been an avid crossword- and math-puzzle solver even during my high school days. That naturally translated into me loving this course and getting interested in cybersecurity. As I researched more and more, I understood that cybersecurity was extremely multi-faceted, and its applications were seen almost across any discipline of engineering and technology. The range of opportunities to learn fascinated me, and I dove right in by proposing a research project on anti-forensics that won me a research fellowship with India's federal banking authority. After that, my industry experience in cybersecurity began almost immediately, following my undergrad studies. I was a part of the Ford College Graduate (FCG) program of 2014, and based on my academic projects and skills, my first assignment was luckily with the Cyber Defense team at Ford.

My Advice: Cybersecurity is easily one of the broadest disciplines of study that I know of. Anyone interested in entering the field may want to first explore the different tracks or areas of focus. A great starting point would be to explore different roles and specialty areas as defined by the National Initiative for Cybersecurity Education (NICE) framework published by the U.S. Department of Homeland Security. It covers both top-down and bottom-up methods to approach a cybersecurity career and also lists the required skills you need to develop for every area of focus. For hands-on experience,

I highly recommend capture the flag (CTF) events, one of the best ways to develop practical skills in computer security, because you get to immerse yourself through problems in multiple focus areas at once. It's also one of the best ways to meet like-minded people and improve collaborative skills.

Fun Fact: I have written a whole book of laterally inverted letters by hand (a.k.a. Intentional mirror-writing).

Liat Hayun

Vice President, Product Management
Palo Alto Networks

Years in Cybersecurity: 10+

"I started out in physics and math, but I took a university course about cryptography and was excited by how our most important assets (e.g., bank accounts, personal details) can be compromised by attackers—and what we can do to protect them. I was hooked!"

A Day in the Life: I lead the Product Management team for Endpoint Security. My team is in charge of defining the strategy and roadmap for the product, based on the feedback we get from customers and the solutions we identify.

How I Got Started in Cybersecurity: I actually got into computer science and cybersecurity by accident. I started out in physics and math, but I took a university course about cryptography and was excited by how our most important assets (e.g., bank accounts, personal details) can be compromised by attackers—and what we can do to protect them. I was hooked! My first job in the cybersecurity arena after college was as a software developer in the army. The longer I'm in this field, the more I become convinced that this was the right path for me. I enjoy the level of excitement around the technical aspects of the job, knowing that a few keystrokes can turn into a compilated software program that protects the Internet. I also like learning how the products we're developing are preventing cyberattacks each day.

My Advice: Once you understand what computer science is and how it works, the next thing you should wonder about is how can it be abused and what can be done to stop that abuse. Keep asking questions, and be curious about how things work and how can they be improved. The field of cybersecurity is always changing and developing. If you want to be successful, don't ever stop learning.

Fun Fact: I only got into cybersecurity after I was mandated to take a class in computer science, which in turn piqued my interest. Ten years later, I actually went back to my university advisor and thanked him for making me take that one course. It changed my entire life.

Alex Krepelka

Senior SOC Engineer
Palo Alto Networks

Years in Cybersecurity: 5

"My advice to those interested in cybersecurity is to look for ways to learn security by yourself, don't look for someone else to teach you."

A Day in the Life: My job is to detect successful attacks on the company, investigate compromises, and come up with new ways of finding evil on our network.

How I Got Started in Cybersecurity: I became interested in cybersecurity when I got a virus on my computer when I was little. My dad worked in IT, so I got access to the Internet pretty early in life. I was downloading a song one day and did not realize it had a .exe extension. When I went to play the song, my system was immediately compromised. The attacker took complete control of my system, including my mouse, keyboard, webcam—everything. I became quite curious as to how all of this happened, so I began looking into how people make malware. This led me to some blogs on writing python, and I have been deeply interested in everything security ever since.

My Advice: My advice to those interested in cybersecurity is to look for ways to learn security by yourself. Don't look for someone else to teach you. It will ensure you understand each subject thoroughly. Take advantage of the Internet, hacking forums or IRC, books, just breaking stuff, and testing.

Fun Fact: I actually got my first real security job from a posting on Reddit.

Xiaobo Liu

Principal Software Engineer
Palo Alto Networks

Years in Cybersecurity: 2

"I knew this was the right career path when I took a security training and found out there are many ways to break into a system. At that moment, I knew I was on the right track to both have fun and make an impact."

A Day in the Life: As a software engineer, I build tools to support the Information Security team to scale on security logs and threat analysis.

How I Got Started in Cybersecurity: I started in cybersecurity by working in different domains such as Operating System, iOS, AWS® Cloud, and Payments. Security is a vertical area for all those domains. Security is continuing to become more and more important with the Internet, mobile, and IoT (Internet of Things). I am confident the necessity and impact of this space will only continue to grow. I knew this was the right career path when I took a security training and found out there are many ways to break into a system. At that moment, I knew I was on the right track to both have fun and make an impact.

My Advice: Stay curious and continue learning new ways to problem solve. I also recommend sharpening your communication skills with people across multiple departments, including IT, DevOps, Product Management, and more.

Fun Fact: I enjoy being the treasurer for my son's Boy Scouts pack.

Adam Schindelar

Staff Red Team Engineer
Palo Alto Networks

Years in Cybersecurity: 6

"I always had a curious urge to get things to do what they were not necessarily made to do. When I was about 10 years old, I found out an unintended way to make myself an administrator on a gaming server for a popular online game."

A Day in the Life: As a member of the Red Team, my primary responsibility is simulating adversary attacks against the organization. I help identify gaps and deficiencies impacting the enterprise security posture and readiness. Specifically, this can include logical network, social engineering, and physical security elements.

How I Got Started in Cybersecurity: I always had a curious urge to get things to do what they were not necessarily made to do. When I was about 10 years old, I found out an unintended way to make myself an administrator on a gaming server for a popular online game. I had no idea what I was really doing, but years later I learned it was essentially a trivial buffer overflow-type attack that would restart the server. I then begged my mother to go out and purchase me a book on ethical hacking. At the time, I could not comprehend anything in the book—but was still mesmerized. After studying computer science in college and spending a short time in the software development world, I knew security was where my heart was. I joined a small information security organization and spent the majority of my career in the consulting world.

My Advice: If you're interested in cybersecurity, first get your feet wet with software development, network engineering, and system administration. Cybersecurity is an extremely large field and has many smaller pieces and parts. However, having a broad general knowledge of "security" is needed for any security specialty. Specifically, for offensive security, look into online capture the flag events, bug bounty programs, and certifications like the OSCP (Offensive Security Certified Professional). These environments allow you to get hands-on experience while developing an attacker's mindset. Combine this with fundamental knowledge and a little bit of "art," and you can be successful in this field. Learning a tool or how to exploit something can be taught, but the most important thing in this area is one's mindset. Always be asking questions—where is the critical data, and how is it being protected? Finally, become active within the information security community. Attend local conferences and reach out to people who are discovering cool tactics, techniques, and procedures (TTPs).

Fun Fact: I like to buy unique art when I travel to various places—"unique" in the sense that it's usually pretty weird.

Rudy Ortega

Senior Security Engineer
Palo Alto Networks

Years in Cybersecurity: 17+

"Get hands-on. If you have the passion to learn security, there is no better way than to do it yourself. That's how I know a lot of what I know—setting things up, breaking them, and understanding how things work. Unless you work out these problems on your own, you won't fully comprehend what is going on."

A Day in the Life: I do several things in my job. I work on the Security Operations team, and I perform monitoring and responses to alerts. We create different alerts, depending on what threat activity we are looking for. We analyze threats to see if they are malicious. I perform incident response and forensic analysis. I also work across departments to ensure we are using optimal configurations and best practices.

How I Got Started in Cybersecurity: While I was in college, I took some programming and computer science classes, but my major was actually biology. I was always interested in computers, and while I was in school, I taught myself Linux. After graduation, a friend recommended me to my first job in cybersecurity because they needed people who knew Linux. I always had curiosity around computers and how they worked—and how you can hack them. At my first job, I worked my way up from technical support, and I learned quite a bit about the product and about the end user. It wasn't until about 2007 that I got more into the information security side of products. I went from being a product specialist to a malware specialist. That's when I learned more about the defensive side of security versus the offensive side. That transition was exciting. On any given day, I was helping clients through difficult issues, and I enjoyed responding to the client's needs. Being able to understand malware also really piqued my interest.

My Advice: Get hands-on. If you have the passion to learn security, there is no better way than to do it yourself. That's how I know a lot of what I know—setting things up, breaking them, and understanding how things work. Unless you work out these problems on your own, you won't fully comprehend what is going on. It is also important to have strong people skills for a successful career in this field. Imagine the environment in an SOC—you are in a room with people all day. If you don't learn those interpersonal skills and bring them to the office, you're not going to be able to survive in that room. We all have good days, bad days, and you have to be able to deal with that. We also work with internal clients and need to understand their concerns and issues to solve them.

Fun Fact: I enjoy trail running, especially half-marathons or longer. I also love the mountains, backpacking, and just being outdoors.

Chapter 2:
Sharpen Your Soft Skills

Jen Miller-Osborn

Deputy Director of Threat Intelligence, Unit 42
Palo Alto Networks

Years in Cybersecurity: 20+

"As difficult as it can be to put yourself out there and talk to people currently in the industry, it is invaluable. If it helps, practice your 'elevator talk' in advance, even if only to yourself in a mirror. I'm a total introvert, and this has been one of the hardest things for me and is something I still work on."

A Day in the Life: I spend the majority of my time performing research, either for something I'm writing or for technical edits of Unit 42 blog posts before publishing. I also travel to conferences and visit customers to discuss Unit 42's research, the importance of freely sharing threat intelligence, our new playbooks, and the importance of women and diversity in tech.

How I Got Started in Cybersecurity: I've always enjoyed puzzles and figuring out how things work. Some of my favorite toys growing up were precursors to modern computers. Working in cybersecurity is just the organic growth of my interest and long-standing hobby. When I got started in the field, it was before "cybersecurity" was a word or there were college degrees in it. There weren't even many technical certifications in existence. I was active duty Air Force and fortunate enough to be selected to train in this new field. I volunteered for it. I thought, since I liked computers and intelligence analysis, it had the potential to be a lot of fun—and it has been!

My Advice: Take classes, go to conferences, and network. Most people in cybersecurity are happy to share what they do and enjoy hearing about what others do and what interests them. GitHub is a great place to showcase projects, whether work-related or hobby, and a way for potential employers to find you. A LinkedIn profile is also important. As difficult as it can be to put yourself out there and talk to people currently in the industry, it is invaluable. If it helps, practice your "elevator talk" in advance, even if only to yourself in a mirror. I'm a total introvert, and this has been one of the hardest things for me and is something I still work on. People in this field tend to be friendly, I promise!

Fun Fact: I started studying foreign languages in fourth grade.

Bryan Lee

Unit 42 Threat Researcher
Palo Alto Networks

Years in Cybersecurity: 10+

"I established key relationships along the way that definitely helped progress my career. As tech professionals, we don't always focus a lot on personal relationships; there is a focus on the hard skills. However, I think my communication and interpersonal skills are what really got me into my first big security position as a Junior Analyst at NASA."

A Day in the Life: My whole team revolves around threat intelligence. We are generally at the forefront of threat intelligence research. We are looking at things that nobody else has looked at before. That includes nation-state adversaries, criminals, and everything in between. When we find interesting things in relation to this space, we publish it to the world.

How I Got Started in Cybersecurity: I had a huge interest in cybersecurity back when I was 12 years old. I started hacking, and it just piqued my interest. The capabilities of computers, networking, the security, was all very interesting to me. I started college in 2003 at San Jose State University with a major in marketing, but towards the end of college I realized that wasn't the right career for me. Since I always had an interest in computers, I accepted my first job after graduation as a low-level admin on a supercomputing center at NASA. Being there—and being back around technology—brought me back to what I loved originally. I continued to expand my security skills just by hacking to learn how everything worked and manipulating things to make them work the way I wanted. I established key relationships along the way that definitely helped progress my career. As tech professionals, we don't always focus a lot on personal relationships; there is a focus on the hard skills. However, I think my communication

and interpersonal skills are what really got me into my first big security position as a Junior Analyst at NASA.

My Advice: If you are really interested in something, just start working at it. I'm very much a hands-on person. I have actually only taken one security course. I only have one certification, and it really wasn't for me. To learn, I ask coworkers, and I go on different websites. The Internet is truly a wealth of knowledge and stays up to date as the technology changes. For me, it's learning by doing and having the enthusiasm to find out an answer. Always ask, "Why?" That's the simplest piece of advice I can give, and it just extends to everything. At the end of the day, curiosity is the end to everything. It's important to understand that there is no one direct path into anything, and security is no different. You don't have to be a threat researcher or reverse engineer; there are all sorts of careers in this field. Just having an interest in this career in general is a great start.

Fun Fact: When I was a kid, I wanted to be a NASCAR driver, but then I realized you have to basically sit in an oven for eight hours, and that wasn't for me.

Guang Wang

Senior Manager, Security Tools, Security Engineering
Palo Alto Networks

Years in Cybersecurity: 11

"Look for people around you to be mentors. Practitioners do a lot of things that you cannot find in books or online, and you can learn from their experience. It's very important for you to reach out proactively. Don't wait for anyone to reach out to you. If you are proactive, it's highly likely that those who are more experienced will be happy to assist you."

A Day in the Life: My team performs engineering support for all functions within various business units in the company and for the Information Security group, including operations, GRC (i.e., governance, risk, compliance), architecture, engineering and IT. We develop homegrown security tools and manage commercial solutions and programs to support the security initiatives for the organization.

How I Got Started in Cybersecurity: As an undergrad, I studied computer science, but there weren't many courses around cybersecurity. During my master's program, I accepted a security internship position at eBay and helped them build their first security operations center (SOC). Until that position, I had imagined that I would just be starting as a software developer and programming at a computer.

My Advice: We face new challenges every day in cybersecurity, which is exciting. When you work in a corporate environment, you have to continually improve your skillset across the board. You have to be self-motivated to always learn. You have to be passionate about digging deeper, not just touching the surface. To understand the technology in real life, you have to get hands

on and talk to experts in the field. Look for people around you to be mentors. Practitioners do a lot of things that you cannot find in books or online, and you can learn from their experience. It's very important for you to reach out proactively. Don't wait for anyone to reach out to you. If you are proactive, it's highly likely that those who are more experienced will be happy to assist you. In Silicon Valley, we do need lots of programmers with top technical skills, but I want to remind people not to ignore opportunities to improve your soft skills too. Once I learned that a big chunk of the responsibility in security was communication and working with people, that was very appealing to me. As an international student, working in this field made me much braver. It forced me to talk to people, and I learned so much from those engagements.

Fun Fact: I did my master's in New Hampshire. I really love and miss the cold weather and the snow.

Jamie Fitz-Gerald

Product Line Manager, R&D

Years in Cybersecurity: 8

"Having a strong network is extremely beneficial. When someone knows you're great and recommends you, it can make all the difference."

A Day in the Life: As a product manager, my job is to define the way our products work from a technology perspective. We define the roadmap of where the products go and how they work. A big part of my job is understanding what our customers need, what problems they are trying to solve, and trying to turn that into features and products that solve those problems.

How I Got Started in Cybersecurity: I studied computer engineering and computer architecture. After college, I worked for several years at a defense contractor, and later I was recruited to my current company by a friend and former colleague. I didn't have a strong security background at that time, but based on my friend's strong recommendation, they took a chance on me. Networking is really what got me here. Since I did not have a background specifically in security, I got a lot of on-the-job training when I started. I had to learn quickly because you need to be an expert in your product when speaking to customers. I sat down with the leads in every area of the product and had them walk me through exactly what they were working on. In addition to that, I had to really get hands on and use the product, and also spend time with customers while they were using the product. Because technology changes so fast, it is essential that everyone is continually learning. I have Google Alerts set up for any news about my company. It's one of the things that I look at every single day.

My Advice: If you have the drive and a desire, then there is a job for you in cybersecurity. The gap between the number of jobs available and the number of qualified people in this field is so wide—and only getting wider. Having a strong network is extremely beneficial. When someone knows you're great and recommends you, it can make all the difference. Use conferences to meet people, make a connection, and continue to build your network. Lastly, you need to be bold. Even if your background isn't an exact fit with a specific role, let your passion guide you. *I'm here because I'm hungry. I'm here because I want to be in this industry.* That's the person I want to hire.

Fun Fact: When I was growing up, I came from absolutely no technology background. I got my first computer as a junior in college. I learned everything about computers after I took my second engineering class and graduated with a degree in computer engineering.

Matt Johnston

Senior Manager, Threat Intelligence, Information Security
Palo Alto Networks

Years in Cybersecurity: 18

"Do everything with excellence. Apply your best to your work, own it, and take full responsibility for your part. Excel at what you do, and let the results speak for themselves."

A Day in the Life: I research cybersecurity-related threats, including the people, tools, and tactics that represent the bad stuff of the Internet, and practice defeating them. I share my knowledge and experiences with the Information Security team and help them defend against those same threats by influencing strategy, helping to guide technology selection and adoption, and helping define processes that enable successful defense. My goal is to combine research, engineering, and operations into a solution set that solves real cybersecurity problems.

How I Got Started in Cybersecurity: Before I was hired into the industry, I knew almost nothing about cybersecurity. I was originally hired as a Level 1 helpdesk operator for a managed security service provider (MSSP). When I was originally offered the role, I literally thought "computer security" (as it was called then) meant I would be a physical security guard for computers. Once I started and was immersed in the space, I found that it was incredibly interesting, challenging, and it turned out to fit well with my skills at problem-solving, analytics, and solution development. It was a natural fit, but I didn't realize that until after I started working in cybersecurity. Even before that, at my first job that I got when I was a senior in high school, it was really simple initially. I managed support calls, coordinated technical support for service requests and trouble tickets, and managed security incidents. I was immersed in cybersecurity and networking, not in a technical capacity at first, but tracking and reporting on the work of analysts and engineers within a SOC exposed me to many aspects of the cybersecurity world. From there, I joined the technical team as an analyst, then engineer, then architect, then innovator.

My Advice: Whatever your final career path, do everything with excellence. Apply your best to your work, own it, and take full responsibility for your part. Excel at what you do, and let the results speak for themselves. I learned the most from people around me and the work assigned to me. If you have interest in this field start with an IT/networking job, practice cybersecurity on the side (at home if needed), and seek opportunities to engage and support cybersecurity teams. I quickly recognized individuals who represented "the experts," and I engaged them with humility. I would ask them questions, seek their advice, and apply what they offered me. I volunteered for assignments, worked late hours and attended voluntary internal trainings. All

of this exposed me to people and experiences that sparked my interest, and then I replicated what I saw. My work ethic also caught the attention of those I had pegged as the "experts," and in return, they began to invest in me.

Fun Fact: Although I have never served in the U.S. military, I am an honorary member of the crew of the USS Salt Lake City, a Los Angeles-class fast-attack submarine, having been fully submerged in the depths of the ocean and participated in exercises while underway.

Lior Zadka

Senior Security Engineer
Palo Alto Networks

Years in Cybersecurity: 15

"One of the skills that has been most helpful to me is that I know how to connect with people. Interpersonal skills and positive relationships with colleagues are essential to helping move toward the goal of keeping employee and company data secure."

A Day in the Life: My role consists of two sets of responsibilities. First, I am a part of the Security Engineering team, helping to manage several products designed to keep employees and our data safe and secure. Second, I take care of information security responsibilities for audit and for the company's Tel Aviv site. This includes security awareness, managing SOC alerts, as well as architectural and governance issues.

How I Got into Cybersecurity: I worked at Israel's largest Internet service provider as a university student. The tech environment was really appealing to me. As I advanced into management, I became fascinated by security. Eventually I moved to a position that was dedicated to information security, and I've been focused on this ever since. In school, I studied computer science, but I'm not the type of person who could be a programmer. When I saw the cybersecurity career path, I realized that is the path I wanted to take. I tried to learn all I could to become the best that I could in my area of expertise. I became a resource and support to coworkers who had questions. I always wanted to know more and more, and I liked to solve hard problems. Also, I naturally enjoy customer service and helping others solve problems. Security gave me the opportunity to provide a service in a very interesting field.

My Advice: One of the skills that has been most helpful to me is that I know how to connect with people. Interpersonal skills and positive relationships with colleagues are essential to helping move toward the goal of keeping employee and company data secure. I try to connect with people by talking about non-work topics before moving into what we need to discuss. I try to be as friendly as I can, and people appreciate it. If you are interested in learning more about security and think this may be a career path for you, start by learning how to protect yourself. Configure a firewall at home. Learn how things are done. Read about the risks. We need to know that cyberthreats can hurt us—but that we can protect ourselves. You can work on building a network at home and building controls in that environment. If you are interested and passionate about it, you can continue with it and pursue a career. If you choose to pursue a career in security, you will never stay in the same place; you will always be challenged.

Fun Fact: I have two first names. My first is Lior; the other is Raphael, which is my grandfather's name and what everyone called me growing up. When I joined the Israeli army at age 18, everyone started calling me "Lior" exclusively, and that's the name that I use today with everyone outside of my family.

Mannie Martinez

Corporate Sales, Emerging Technologies
Palo Alto Networks

Years in Cybersecurity: 2

"Network outside of your direct team and organization. You never know who you'll meet. Find a mentor willing to hold you accountable to yourself. Work on your communications skills."

A Day in the Life: At work, I help Silicon Valley and San Francisco startups combat and overcome the economies of scale, automation, and sophisticated techniques leveraged in modern cyberattacks. As an Emerging Technologies Representative, I am an advocate for and evangelist of our latest innovations. This includes communicating regularly with our customers, as well as partners in the channel and distribution. During a prospecting or an opportunity-driving day, I'll often make 25–60 calls and send 50–250 emails. All this activity leads to customer meetings, which lead to opportunities to help customers, which lead to pipeline, which leads to bookings, which lead to our mutual success. On a great day, I'll have as many as five customer meetings to learn about their challenges and demo our technologies. During downtime, I'll read up on our tech and trends in our industry, or I'll conduct strategic research on customers and prospects.

How I Got Started in Cybersecurity: I was recruited to Palo Alto Networks by a friend of mine who especially appreciated my passion for helping others. Helping others is a very important theme for me. It all started when a high school bully twice my size targeted me on one occasion and just wouldn't give up. I stood up for myself with everything I had but was simply overpowered by his brute force. A good friend of mine closer to his size stepped in and, together, we overcame the attack. I eventually forgave the bully and made a promise to myself to stand up for the underdog as my friend did.

My Advice: Embrace your organization's mission and commit it to memory verbatim. At Palo Alto Networks, our mission is: "Cybersecurity partner of choice, protecting our digital way of life." We literally keep organizations online and hackers out of our major infrastructure, not to mention all the cool applications that are changing the world. Embodying this mission will accelerate your learning on the job. When you encounter the tougher challenges in cybersecurity, it will carry you through. As you carry yourself around the office and in the field, it will shine from within—and your customers and colleagues will feel your energy and passion. Network outside of your direct team and organization. You never know who you'll meet. Find a mentor willing to hold you accountable to yourself. Work on your communications skills. At our company, we have not one but two Toastmasters clubs to continually hone our speaking and leadership skills.

Fun Fact: I'm a bit of a fitness and nutrition nut. I have a nutrition corner on my desk, and when I'm not studying our latest cybersecurity innovations, I'm learning about neuroplasticity and tendon strengthening.

Chapter 3:
Embrace a Leadership Mindset

Rinki Sethi

Vice President, Information Security
IBM

Years in Cybersecurity: 15+

"Cybersecurity has come a long way in the past decade, and I'm inspired by what the future holds for all of us."

A Day in the Life: One day may seem insignificant if you consider it in the context of an entire career. But, if you break down one day into its parts and possible experiences—such as making new connections, brainstorming unique methods of data visualization, and refining the decision-making process—what happens in one day can change the outcome completely. That's why my team and I make the most of each and every day. I'm very proud that I get to work with a team of amazing security experts who, on a daily basis, inspire one another to come up with different ways to prevent successful cybersecurity breaches. We leverage cutting-edge attack techniques and tools to define and prioritize threat areas, and we work side by side with colleagues within and outside of the Information Security department to close gaps in enterprise security. We are responsible for building out our security operations center, which includes threat management, threat intelligence, security monitoring, and incident response functions. We also drive our red team/blue team practice, our attack and defend capabilities, and security education and awareness for the company. So much is possible in just a day, and I'm excited that every day can offer a challenging and rewarding experience in cybersecurity.

How I Got Started in Cybersecurity: Cybersecurity has come a long way in the past decade, and I'm inspired by what the future holds for all of us. For me, since the beginning, this has been a journey that has been much more than I could have imagined. Thinking back to when I first got started in cybersecurity, as a graduate of the University of California at Davis with a degree in computer science engineering, I remember a conversation that changed my career path. I was telling a hiring manager at a school career fair about my interest in cryptography, and soon after, I had an opportunity to work in information protection. Over the years, I've continued to learn about cybersecurity from my teams, colleagues and mentors, and my list of topics of interest has really grown! I find that the possibilities in cybersecurity have grown tremendously over the years. Organizations are innovating in how we need to operate and do business. The amount of data has increased rapidly, and as cybersecurity practitioners, we get to help protect our organizations from the bad guys.

My Advice: To anyone beginning a career in cybersecurity, I think it's so important to find something you're passionate about. Then, find experts who are working in these areas, connect with them, and be open to learning from their experiences and insights. Luckily,

throughout my career, I've had many great mentors, sponsors, and inspirational leaders. Building a strong network will be key as you begin your career and at every step of the way. When I have an opportunity to introduce young kids to what cybersecurity is all about, share what it's like to work in this field, and talk about both the technical and people skills required to get started and be successful, I see how curious they are and open to exploring more. I think that, if we go to our schools and encourage students to get hands-on experience, we'll build a strong cybersecurity workforce—and leaders—to tackle tomorrow's challenges.

Fun Fact: I enjoy watching sports with my family and cheering for our favorite teams.

Lucas Moody

Chief Information Security Officer
Palo Alto Networks

Years in Cybersecurity: 18

"In cybersecurity, our responsibilities are equal parts thought leadership, business innovation, and constantly challenging our assumptions about our understanding of the digital world."

A Day in the Life: There's no question about it: Information Security needs to be understood as a competitive advantage in this digital age that we live in—as cyberthreats impact all organizations, of all sizes, wherever they operate. In our connected economy, my role as CISO means I work closely with my team to develop a security culture that permeates our organization, enabling our business to continue to thrive while growing securely. On any given day, we work to understand the threat landscape and monitor our risks to make the right technology investments—and develop processes and our people—to ensure that we stay ahead of the game. In cybersecurity, our responsibilities are equal parts thought leadership, business innovation, and constantly challenging our assumptions about our understanding of the digital world. The foundation on which my team is built consists of strong technical and operational roots, and a true passion for protecting our digital way of life.

How I Got Started in Cybersecurity: I was a hacker in the classic sense where I was curious about everything, and I tried to explore, break, and fix every piece of technology that I got my hands on. I learned by doing and experimenting with everything, picking it all apart to really understand how it worked. Early on, I was interested in tech in various forms, including telecommunications, raw technology, and software development. In college, I studied computer science, and I was particularly fascinated with how computers talked to one another. My interest in networking quickly expanded into security because as devices become more interconnected, they become more accessible, making trust an important aspect of connectivity. Back then, there were very few laws around cybersecurity, and every problem that we came across was something that had never been seen. It was like setting sail for the New World, with cybersecurity practitioners as the explorers who looked to experience the new and unknown.

My Advice: My advice is to look for opportunities that will allow you to apply your varied skills, experiences, and mindset. Teams and leaders who will invest in you and ensure your continued growth and learning will be well-worth searching for. Follow leaders who want to build out a team where candidates may not have the exact skills and experience at that moment; instead, these leaders seek team members who have a strong passion for learning, a keen eye for detail, and excellent reasoning skills and analytic capabilities—as well as strong communication and collaboration

skills. If everyone on a team brings diverse skills, experiences, and backgrounds, then when it comes time to solve unexpected challenges, the solutions would be as equally diverse and innovative. As you advance in your career, be sure to share any observations you have about existing people, process, and technology that might not be as effective, and call to the surface issues that can affect risk. Your leaders and team will appreciate and benefit from your insight!

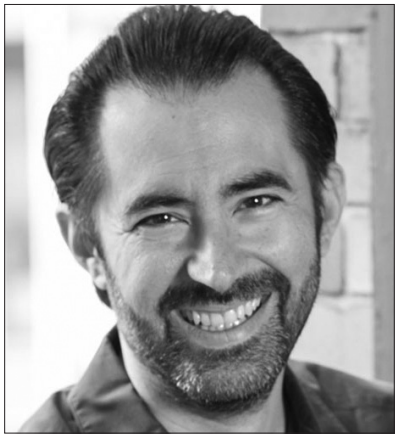
Fun Fact: My first computer exploration vessel was a 286-12 with 512K memory and a 20 megabyte hard drive with a 1200 baud modem. And I loved it.

Elias (Lou) Manousos

Co-Founder and Chief Executive Officer
RiskIQ

Years in Cybersecurity: 20

"Unlike other computer systems where each problem has a solution, cybersecurity is a continuously evolving game in which your opponent is the cybercriminal. These criminals are always adapting, so you need to adapt too."



A Day in the Life: I am the CEO of RiskIQ®. Our vision is to redefine the global standard for security programs by delivering exceptional protection beyond the firewall. My way of delivering this to the market is organizing the infrastructure and mapping the interconnectivity of the Internet into a "security graph." We use this graph to catch cyber threats and attackers as they interact with the Internet. Also, I am currently very interested in the confluence of security and privacy and the debate around Internet tracking. I believe some of the work being done to improve online privacy tells you quite a bit about the attacks taking place.

How I Got Started in Cybersecurity: I grew up in Chicago and had a fascination with Al Capone, organized crime, and the law enforcement actions that unraveled it all—you know the saga of Eliot Ness and "The Untouchables." As a self-taught programmer with deep knowledge of computing, I recognized that a system could not function properly without confidentiality, availability, and integrity. I was very interested in the Internet, and as the Internet grew in importance, I watched how criminals could "hide in the shadows" and use it to carry out attacks and abuse Internet systems at scale, not unlike those old gangs in Chicago. I was working at a national lab while studying physics during the same year Shimomura helped catch Kevin Mitnick. I saw the potential of the Internet for both good and bad, and decided to drop out of school to develop software. It wasn't long before my focus shifted to cybersecurity.

My Advice: Do you like to play games? At its most basic level, cybersecurity is a game, and your greatest resource is a passionate curiosity in understanding the rules and tactics. Unlike other computer systems where each problem has a solution, cybersecurity is a continuously evolving game in which your opponent is the cybercriminal. These criminals are always adapting, so you need to adapt, too. Understanding the motives and tactics used to abuse systems and deceive people first requires a desire to hunt bad guys or "chase rabbits." When you dig even deeper into these attacks, what you find will often surprise you and fuel your interest in cybersecurity and desire to learn more. Start by taking the time to research the successful attacks and the weaknesses they exploited. Security companies and independent researchers often write about these in great detail on their blogs. When you read into many of the successful attacks taking place

today, it's alarming how simple they are. Simple attacks are common, and their coverage provides excellent info for those looking to learn about the industry and develop an interest in the space.

Fun Fact: Most people know I love boats, but lately, I have been trying to fish in the San Francisco Bay. So far, I'm better at catching cybercriminals than fish.

Danielle Kriz

Senior Director of Global Policy
Palo Alto Networks

Years in Cybersecurity: 16

"Don't be shy about getting into the cybersecurity field; it's much wider than people think. Careers are not just in coding, and they're not just in hacking. They are in everything from marketing to law to communications to policy. If you're smart, motivated, and interested, there's always going to be a place for you."

A Day in the Life: The focus of my job is interfacing with government officials from a public policy perspective. My team works with government officials around the world, and I, personally, focus on key markets throughout Europe and Asia. We track which laws are being developed that might regulate cybersecurity, and which policies are being developed related to cybersecurity, including data issues, cloud, standards, or anything else that impacts our company or customers. We focus on three main areas: building our brand, monitoring and reporting internally on laws and regulations, and advocating for laws and regulations that align with our interests. Our work also helps open doors. If one of our senior executives is visiting a country or region and we want to get a meeting with officials such as president, prime minister, or cabinet heads regarding cybersecurity policy, it always helps when we know people at the staff level who can recommend us as a leading resource.

How I Got Started in Cybersecurity: I actually got into this field completely serendipitously. I have my master's degree in international trade, and I got interested in the technology industry while in graduate school. I began my career working for the U.S. government on trade agreements that impacted the import and export of technology products. This was the early days of the Internet and e-commerce. That sector of countries' economies was beginning to dramatically grow, and governments around the world were wondering what their policy responses should be and if regulations were necessary. The U.S. government's official position was not to regulate these areas, and it was part of my job to keep global markets open for U.S. companies that made the technology that supported the Internet and e-commerce. Tech companies want to build one product and sell it everywhere. They don't want to build to 150 different standards, or have governments dictate what technology to use or which standards to build to. The market best drives innovation, and we tried to encourage other governments of the benefits of that approach. In the early 2000s, some governments were beginning to regulate cybersecurity, which we also looked at, in part, through a trade lens. I negotiated with other countries to keep markets open for U.S. companies that built cybersecurity products, and that's what got me hooked on this field.

My Advice: Don't be shy about getting into the cybersecurity field; it's much wider than people think. Careers are not just in coding, and they're not just in hacking. They are in everything from marketing to law to communications to policy. If you're smart, motivated, and interested, there's always going to be a place for you. Building my professional network and asking questions definitely have helped me to learn and progress in my career. When I was working in government and new to this field, I could reach out to individuals in different government departments to get answers I needed. Cybersecurity is so broad that it's helpful to have different subject matter experts you can talk to directly about an issue. I've been fortunate to build up a great network over the years, and I'm not shy about asking them to share their expertise.

Fun Fact: I lived in Tokyo, Japan, between college and graduate school. I enjoyed teaching English, and I think it was where I really discovered how much I like being overseas and bridging cultures.

Rick Howard

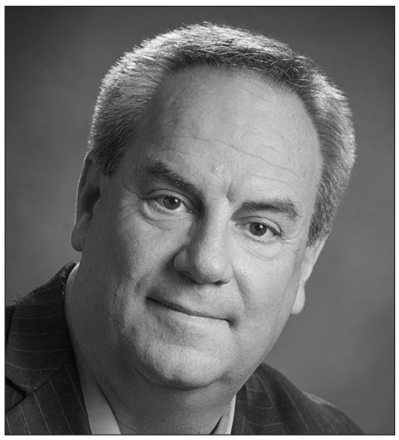
Chief Security Officer
Palo Alto Networks

Years in Cybersecurity: 30

"Having mentors is the most important thing. I've had many mentors who have helped me, and now I try to mentor as many people as can stomach me! You get lost in the wilderness out there; you need to seek out mentors who have done things that you admire. As you move up the chain, take time to mentor other people."

A Day in the Life: I have three jobs at Palo Alto Networks. First, I'm in charge of overall security for the company. Second, the Unit 42 threat intelligence team works for me. Third, I get to go out and share what we're learning with the world. What I really like about the job is that it changes all the time. There is always something new to learn—some dastardly thing that some adversary did, and then some brilliant thing that a white hat hacker came up with to counter it. I love that part of the job.

How I Got Started in Cybersecurity: I was always interested in computers, mostly because I'm a gamer, and I wanted to make games. I joined the Military Academy and went into computer science because that was as close to creating video games as I could get. The military also sent me to graduate school. I was going to be an IT professional, but about halfway through grad school, The Cuckoo's Egg was published, and that book changed my trajectory. The book was written by a Berkeley astronomy professor who worked for a year in a UNIX lab and discovered the first evidence of the first public cyberespionage campaign to break into universities—so they could break into government systems. I found it completely fascinating, and interestingly, all the things the author grappled with in this book, we are still dealing with today. I got an opportunity during my career in the military to run the Army CERT (Computer Emergency Response Team).



They were in charge of coordinating offensive and defensive operations for the U.S. Army®.

My Advice: Having mentors is the most important thing. I've had many mentors who have helped me, and now I try to mentor as many people as can stomach me! You get lost in the wilderness out there; you need to seek out mentors who have done things that you admire. As you move up the chain, take time to mentor other people. By next year, there will be a 2 million-person shortfall in cybersecurity employees.[8] That means we are close to having 2 million jobs in the industry that are unfilled. Women are only 25 percent of the technology workforce now,[9] and only 11 percent of the cybersecurity workforce.[10] If we do the math, as leaders, we have a lot of opportunities to hire for different experiences, skillsets, and perspectives. That is something I am preaching everywhere I go.

Fun Fact: I grew up in Lead, South Dakota —a very small town. I closed the door when I left, so I'm not sure if anyone is still there. My father was a gold miner and worked in the gold mine that gave the Hearst family its fortune.

8."2016 Cybersecurity Skills Gap," ISACA per the UK House of Lords Digital Skills Committee, January 2016, https://image-store.slidesharecdn.com/be4eaf1a-eea6-4b97-b36e-b62dfc8dcbae-original.jpeg.

9. Ryan Noonan, "Women in STEM: 2017 Update," U.S. Department of Commerce, November 13, 2017, https://www.commerce.gov/sites/commerce.gov/files/migrated/reports/women-in-stem-2017-update.pdf.

10. "The 2017 Global Information Security Workforce Study: Women in Cybersecurity," Frost & Sullivan, 2017, https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf.

Jeff Seifers

Principal Security Engineer
Palo Alto Networks

Years in Cybersecurity: 20+

"At the end of the day, companies are people. You need to figure out how to work with those people. The cybersecurity stereotype of the computer nerd in the corner of the room who doesn't talk to anyone doesn't exist anymore. There is not a position where someone can hide in a cube all day. Push your comfort zone to grow those people skills."

A Day in the Life: I facilitate the implementation of security services, primarily partnering with information technology services to deploy identity access management and privilege access management. I provide security direction and program management support.

How I Got Started in Cybersecurity: I had done basic IT for several years, when security was at the very beginning stages. I found that I wasn't challenged with basic IT, and it became very routine for me, personally. On the security side, I enjoy the adversarial aspect that keeps you constantly guessing.

My Advice: Expose yourself as much as you can to as many areas in cybersecurity when you start out. Look to find the right employer that will give you the ability to experience different facets of the field. There is incident response, network security, application security, and many others. Focus for enough time so that you can make a good decision. At some point, you'll need to apply a degree of focus in order to become very good, given how large the space is. It's good to learn the core fundamentals on how operating and networking systems work and the various layers of security that have been in place for 20+ years. Make sure you understand those fundamentals first before you go playing with the exploit tools. Looking back on my own career, I know that being successful in security isn't about being a subject matter expert on everything. This is a difficult space where you are often sitting and having business risk conversations, trying to influence others to remediate issues on systems or services you don't own. Being a subject matter expert is table stakes. Having strong interpersonal communication and problem-resolution skills are what move you to the next level. At the end of the day, companies are people. You need to figure out how to work with those people. The cybersecurity stereotype of the computer nerd in the corner of the room who doesn't talk to anyone doesn't exist anymore. There is not a position where someone can hide in a cube all day. Push your comfort zone to grow those people skills.

Fun Fact: One of my greatest passions in life is meditation. I am a regular meditator, and I believe it has helped me immensely in the challenging world of information technology and security. I consider it an absolute lifesaver.

Chapter 4:
You Miss 100 Percent of the Shots You Don't Take

Mary Sawyer

Information Security Engineer, Red Team
Palo Alto Networks

Years in Cybersecurity: 1

"Don't take no for an answer. If someone tells you, 'You don't look like a security expert," or that you don't have enough experience, it's their loss. There are so few people in security, there will always be someone out there who is looking for someone just like you. It's just a matter of finding someone willing to give you a chance."

A Day in the Life: I work on the Red Team. Basically, that means I break stuff, usually computers and applications, but sometimes other things.

How I Got Started in Cybersecurity: I decided to take an internship with the Cyber Defense Labs in Dallas just to give security a try, and I ended up loving it. That summer, I did a deep dive into a wide range of topics and technology with the mentorship of a handful of experienced cybersecurity professionals. It inspired me to focus on security topics in school and become an officer in my university's security club on campus. To those just starting out, I would recommend that you join or start your own security club at your college, university, high school, company, etc.

My Advice: My advice is simply to show interest. Regardless of what point you are at in your career, there are always ways that you can show recruiters or other professionals that you are interested in security. Whether it's simply going to security conferences or club meetings, taking a stab at getting some bug bounties, or taking the initiative to work on a personal project related to security, these things will show others that you're interested and motivated to learn. Don't take "no" for an answer. If someone tells you, "You don't look like a security expert," or that you don't have enough experience, it's their loss. There are so few people in security, there will always be someone out there who is looking for someone just like you. It's just a matter of finding someone willing to give you a chance. The key is to find other like-minded people who are willing to answer your questions and guide you on your journey

Fun Fact: I graduated from the University of Texas at Austin and started my first job in cybersecurity before I was 21.

Lauren Che

Security Research Engineer
Palo Alto Networks

Years in Cybersecurity: 4

"I don't think I would've gotten here if I hadn't taken the chance to apply, even though I thought I wasn't ready. Looking back, I think I never would've felt like I was ready or good enough for any security-related position. If something interests you, just apply. The worst thing that's going to happen is that someone is going to say, 'no.' Don't say no for them by not applying."

A Day in the Life: I write IPS signatures to cover the latest vulnerabilities. This involves doing research on vulnerabilities and exploits, and working a lot with an open source packet analyzer and packet captures. You need to know what an exploit "looks" like on the wire in order to write a signature to detect it. One of the biggest challenges of writing network-based intrusion prevention system (IPS) signatures is finding a pattern that strikes a balance between being general enough to detect all the different ways the vulnerability can be exploited, and being specific enough so as not to break our customers' systems. This is my first job in security, so it was a great way for me to become familiar with the different types of vulnerabilities and exploits out there.

How I Got Started in Cybersecurity: I attended a career fair hosted by my university, where I met a hiring manager who referred me for an internship position. I thought I wasn't ready to even go to a career fair since I didn't major in computer science, and I had finished only a few computer science classes at a nearby state college. However, I think the hiring manager was impressed with my enthusiasm for security.

I showed it not only through my spiel but also through my resume. I had taken some fundamental computer science courses after graduating, participated in an InfoSec club, and had done a few small projects on my own.

My Advice: I don't think I would've gotten here if I hadn't taken the chance to apply, even though I thought I wasn't ready. Looking back, I think I never would've felt like I was ready or good enough for any security-related position. If something interests you, just apply. The worst thing that's going to happen is that someone is going to say, "no." Don't say no for them by not applying. To be more prepared, study some of the resources available on the Internet. There are a lot of resources on how to get started, which programming languages to use, and ways to practice common hacking techniques.

Fun Fact: I have an undergraduate degree in molecular toxicology. It's like security, but for the body!

Cynthia Cox

Principal, Governance, Risk & Compliance
Palo Alto Networks

Years in Cybersecurity: 10+

"You will not land your perfect job on the first try because, until you try different hats on, you will not know what your dream job is! Find a job in your field of interest with a supportive team, and things will fall in place."

A Day in the Life: I am a governance, risk and compliance (GRC) professional. GRC professionals require a great breadth of knowledge in each of those three core areas. In governance, I work to define our security posture and measure our progress against these goals. Risk management is the art of balancing security risks with business needs. In compliance, our team works to enable sales through compliance with security/privacy frameworks and legislation, contract negotiations and security certifications.

How I Got Started in Cybersecurity: I did not set out to have a career in cybersecurity. Instead, my career journey has been a series of fortunate accidents that have culminated into where I am today. I started my career in finance as an ordinary accountant with no cybersecurity relevance. I needed to program small macros to automate monotonous accounting tasks. Eventually, I was responsible for configurations in the enterprise resource planning (ERP) system. This led to a career change to work for KPMG, a Big Four accounting firm, during the start of the Sarbanes Oxley 404 legislation, where my knowledge of how configurations and accounting worked together was paramount to understanding how one could manipulate the system to possibly hide fraud. Then, I moved to work in an organization where I was an internal auditor/analyst working on security and privacy audits, such as Payment Card Industry (PCI) and Safe Harbor. Overall, I knew that cybersecurity was the career for me because it is exciting to know that my work contributes to the security of our products and helps our customers be more secure. When a security weakness is remediated, that is one less way for the hacker to compromise the system! The objective of security professionals is to make it as hard as possible for the hacker to breach the system and to limit the damage that they can do.

My Advice: I encourage those who are interested in a cybersecurity career to be open-minded when looking at job descriptions. You will not land your perfect job on the first try because until you try different hats on, you will not know what your dream job is! Find a job in your field of interest with a supportive team and things will fall in place.

Fun Fact: I am a certified sailor and SCUBA diver.

Matt Mellen

Senior Manager, Security Operations Center
Palo Alto Networks

Years in Cybersecurity: 15

"Read all you can and take advantage of all the open source tools that you can play around with. In cybersecurity, what we look for when we hire is: Do you have a passion for cybersecurity, do you have an analytical mind, do you like solving problems?"

A Day in the Life: I lead our security operations center (SOC), which is the mechanism within an organization that handles all of the threat response and mitigation activities. It's the front line for an organization against cyberattacks. My role is to lead the team in all respects, from managing the group of analysts to leading the strategic direction for the SOC.

How I Got Started in Cybersecurity: I have an undergraduate degree in computer science and a master's in digital security. I initially became interested in cybersecurity when I was in a struggling startup, and the websites I created were constantly being hit by cyber attackers. That was my first exposure to attackers. I decided at that point to take my career in the direction of learning more about cyberattacks and getting on the right side of that equation. The whole experience of working at a startup and learning the importance of secure coding was the first time I'd thought about the silent battle between those who are creating useful things in society, and those who are trying to break them. That continual battle was why I thought pursuing cybersecurity would be interesting and rewarding. The fact that it's an ever-changing space in the technology world is very appealing.

My Advice: I think there are a lot of paths to becoming a security professional. Some people take the path of studying for certifications. Another path is jumping in on the educational route. It doesn't matter which path you take, as long as you dedicate yourself to that path. Read all you can and take advantage of all the open source tools that you can play around with. In cybersecurity, what we look for when we hire is: Do you have a passion for cybersecurity, do you have an analytical mind, do you like solving problems?

Fun Fact: I've climbed Mount Shasta (14,000 feet). I've also run marathons and participated in competitive trail running. Exercise is a great way for me to stay fit and to mentally relax.

Muoi Landivar

Security Education & Awareness Lead
Palo Alto Networks

Years in Cybersecurity: 2

"Don't be intimidated. Cybersecurity is constantly changing, so there's always an opportunity to learn."

A Day in the Life: My role is to help employees around the world have an exceptionally strong, active culture of security. I work with our leaders and volunteer community of security champions to design engaging activities, resources, curricula, and events that help employees *learn more, do more,* and *share more* to prevent successful cybersecurity breaches at work, at home, and in the community.

How I Got Started in Cybersecurity: I started in this field because I had a friend who worked in security. I didn't know much about the industry, but my friend recommended me to my current manager, explaining that I might be a good fit with my journalism skills, communications experience, and analytical nature—even though I didn't have experience in cybersecurity. The team and the position turned out to be a great fit for me. I've learned so much about cybersecurity in the past two years. I love that I get to ask my colleagues a lot of questions.

My Advice: I recommend to everyone who may be considering this field to be open-minded to the possibilities. If you're just starting out in your career or trying to make a career change, know that your unique experiences and perspectives can help you to solve problems. Don't be intimidated. Cybersecurity is constantly changing, so there's always an opportunity to learn. If possible, attend cybersecurity conferences and talk to people who are actually working in cybersecurity. It's a very broad field. When I started my career, I wanted to be a journalist, and now I think it's fabulous that I get to work in cybersecurity, where I can use my journalism skills—investigation, research and analysis, and interviewing—to talk with experts and then write about what I've learned, to help others understand more about what they can do to be safe and secure in this digital age.

Fun Fact: Spanish is my fourth language. Learning Spanish really helped me to understand and master my third language: English—and concepts like the subjunctive.

Jake Brunetto

Principal Security Architect
Palo Alto Networks

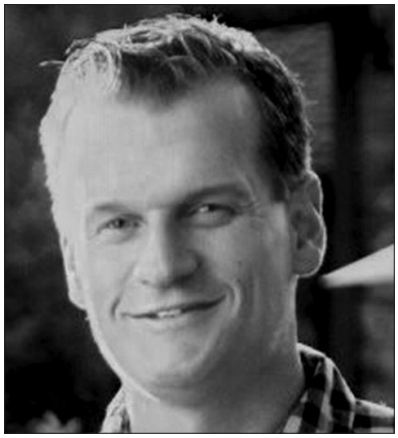
Years in Cybersecurity: 19

"Opportunities abound—put yourself out there and work hard! If you're passionate about the work and love to learn, you'll do well."

A Day in the Life: I'm a security architect. What this means is that I work on building security capabilities in enterprise environments to prevent bad things from happening. Daily work is a mix of technology innovation, partnering and planning, and thinking about things from a threat-centric view.

How I Got Started in Cybersecurity: I got into this field by happenstance. I applied for a free internship opportunity while in college in San Diego. I literally applied without even fully understanding what cybersecurity was. Once I was in front of a SPARC® server, installing BSD and a Gauntlet firewall (look it up), I knew that this was what I loved. It has been a fun journey from those days until now, working with many great people and solving fun challenges.

My Advice: If you're interested in cybersecurity, I recommend that you read a ton and start experimenting with security tools.



Additionally, connect and communicate with cybersecurity professionals, and in general, get started. Use conversations as an opportunity to learn. I try to look at my interactions with my colleagues as an opportunity to learn via their unique perspectives. Opportunities abound—put yourself out there and work hard! If you're passionate about the work and love to learn, you'll do well.

Fun Fact: I live in San Diego, and if I had more free time, I'd surf and practice jiu-jitsu every day.

Kevin Lee

Risk Analyst, Governance, Risk & Compliance
Palo Alto Networks

Years in Cybersecurity: 1

"While many jobs require a deep technical understanding, the main barrier to entry is the ability to think critically and to be open to learning new things. The ability to adapt and work in a shifting environment is critical to succeeding in any technology field."

A Day in the Life: I work with internal stakeholders (HR, Engineering, IT, etc.) to understand their processes and help drive risk remediation or mitigation. Additionally, I perform security assessments on vendors and third parties who may be handling our company's data. Also, when we have external auditors who are certifying our products, I help coordinate meetings between them and the internal stakeholders, and provide requested evidence and information to assist in the understanding of our processes, with the goal of the auditors issuing a report to enable sales.

How I Got Started in Cybersecurity: I first got interested in cybersecurity during my first job as a risk consultant at one of the top global accounting firms. In that role, I was tasked with analyzing IT systems and processes at banks and publicly traded companies to provide recommendations on improvements. From my analysis, I found many of my clients had gaps in information security and were very susceptible to attacks from both external and internal threat actors. While my job was not entirely focused on information security at the time,

I continued to learn and became one of the IT/InfoSec specialists in my office. Later, I left my job with the intent to work for a government intelligence agency. During the period between jobs, I received a message from a recruiter asking if I was interested in applying for a position in information security. After learning about what I would be working on and receiving an offer, I decided to change my plans and come work in the field of cybersecurity.

Take My Advice: While many jobs require a deep technical understanding, the main barrier to entry is the ability to think critically and to be open to learning new things. The ability to adapt and work in a shifting environment is critical to succeeding in any technology field.

Fun Fact: I was born and raised in Honolulu, Hawaii.

Anuj Karnik

Senior Information Security Engineer
Palo Alto Networks

Years in Cybersecurity: 5

"If you are considering a career change, go for it! A lot of people in cybersecurity didn't choose it originally as a career path because it didn't exist 10 or 15 years ago. I've seen people with all sorts of degrees end up in security, and each story is more fascinating than the next. The job market in this field is constantly expanding."

A Day in the Life: I primarily act as the administrator for software that is used for searching, monitoring, and analyzing machine-generated big data. This includes everything from your login to your laptop, your login to the server to firewall logs, and more. All of that gets deposited into software and database, and then the security operations center uses that data to look for red flags, anomalies, and malicious behavior.

How I Got Started in Cybersecurity: I was in grad school, and a friend dragged me along with him to a network security course he was auditing. It turned out that I liked the course much more than my friend. I ended up taking the course and my friend dropped it. I ended up taking several more security courses and then getting an internship in the field. I knew this was the right path for me during my internship when we were running a SOC for a financial firm in Alaska. I found out about an ongoing attack that was originating from Russia but being routed through Estonia. The whole process, catching a malicious attack and investigating the details, was thrilling. During the week when we were working on this problem, I found that, when I got home, I just wanted to head back into the office to continue to work on the issue. That is what convinced me that this was the right direction for my career.

My Advice: Don't just chase big brand names for your resume. Instead, focus on getting the knowledge and pillars right. Those are so fundamental, and if you don't have them mastered as you progress in your career, you will find yourself being sidelined. I realized being at a small company early in my career and "getting thrown in the deep end" really helped me secure my fundamentals, and it's paying me back many times over. If you are considering a career change, go for it! A lot of people in cybersecurity didn't choose it originally as a career path because it didn't exist 10 or 15 years ago. I've seen people with all sorts of degrees end up in security, and each story is more fascinating than the next. The job market in this field is constantly expanding.

Fun Fact: I enjoy cooking and baking. My mom almost had a cake shop when I was growing up, so I was surrounded by cake all the time. More recently, my signature dish is kabobs.

Chapter 5:
Know Your Stuff and Find Your Niche

Prajakta Jagdale

Senior Manager, Red Team
Palo Alto Networks

Years in Cybersecurity: 11

"First and foremost, I recommend finding a focus area. Cybersecurity is a vast field and can quickly become overwhelming if you don't limit yourself to a specific sub-field. Then, get hands-on with the subject."

A Day in the Life: I manage a Red Team program designed to emulate cyberattacks against enterprise networks and predict how well they'll fare against a real attack.

How I Got Started in Cybersecurity: While studying computer engineering, I was introduced to cryptography and its mathematical underpinnings. It instantly fascinated me and prompted me to study information security through a graduate program. During my graduate studies, a co-founder of an Atlanta-based application security company delivered a presentation on web application hacking. I immediately knew that I wanted to know more about it and applied for an internship at the company. It paved the way for the rest of my career in cybersecurity. When I started, cybersecurity was a relatively new field, and there weren't as many resources. I relied heavily on on-the-job training. I was surrounded by some of the most talented individuals in the industry, and I learned as much as I could from them. A few local conferences were also a great source of new and advanced techniques. The rest of it involved setting up experimental labs and trying out my skills. I was given the chance in the last two roles I was hired for because I demonstrated the ability to learn, think, and teach during the interview process. In the field of cybersecurity, where there is such a dearth of

talent, these critical skills can become your winning ticket, in addition to your personal experience and knowledge. Don't be afraid to take a risk because there are plenty of opportunities for course correction.

My Advice: I hope many of you consider cybersecurity as a career path. First and foremost, I recommend finding a focus area. Cybersecurity is a vast field and can become quickly overwhelming if you don't limit yourself to a specific sub-field. Then get hands-on with the subject. If it seems too daunting, try to find a partner you can work with and learn together. It'll give you a significant advantage. But, if that approach doesn't fit you, then read up as much as you can on the topic. This kind of initiative will pay off when you start searching for a job by showing that you are invested in the field. If you do have an opportunity to attend a conference, make sure you connect with some experts and don't hesitate to use them for guidance.

Fun Fact: I'm a *Calvin and Hobbes* fanatic.

Caroline Wong

Vice President
Cobalt.io

Years in Cybersecurity: 13

"Once you find out what type of role you are interested in, look up job openings to find out what kinds of experience and skills you need to get there. Then, begin to build those skill sets and obtain those experiences however you can."

A Day in the Life: I currently work for a startup based in San Francisco that provides penetration testing as a service. I joined a couple of years ago as the 10th employee. In a small company, everyone plays many different roles and performs many different tasks. Some of the responsibilities that I enjoy the most are speaking at industry conferences and hosting executive dinners where I lead roundtable discussions about software development and security. I also run our customer advisory board, which brings an intimate group of our customers together and focuses on strategic planning. Since I joined the company, the team has quadrupled in size, and we are on target to achieve 10x revenue growth. It's extremely exciting to be part of a startup that has found product market fit. Every day there is something new to do and more to learn.

How I Got Started in Cybersecurity: Actually, I never set out to work in cybersecurity. In college, I studied electrical engineering and computer sciences at the University of California, Berkeley. Between my junior and senior year, I had an internship at a large, global e-commerce company in their IT department as a project manager. When I graduated, I reached out to my internship manager, hoping to work for the team full time. There was a hiring freeze in IT, so he couldn't hire me. But, he told me about an entry-level position on the information security team—something I didn't know anything about. The night before my interview, I memorized the Wikipedia page on "information security," and I got the job!

My Advice: The great thing about the security industry is that there are many resources available for people wanting to learn about the field. Some are paid, like graduate degrees, training courses, and conferences. But, others are free or relatively low-cost, like articles, white papers, books, and videos of conference talks online. For someone totally new to the field, I recommend checking out the agenda for different security conferences to discover what topics you are interested in. Then, look up the topics and associated subject matter experts, and go from there! Once you find out what type of role you are interested in, look up job openings to find out what kinds of experience and skills you need to get there. Then, begin to build those skill sets and obtain those experiences however you can.

Fun Fact: Right now, two is the perfect number for me. I have two kids, two dogs, and two cats—double the love, double the fun.

Damilola Longe

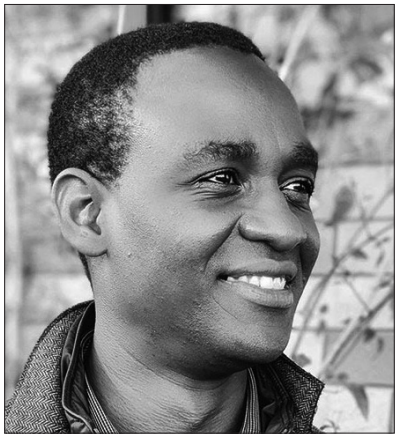
Senior Security Engineer
Palo Alto Networks

Years in Cybersecurity: 10+

"Learn wide early and specialize as you mature. Like a lot of professions, cybersecurity is wide-ranging, so a general exploration of the field early on can be a significant benefit as you begin your journey."

A Day in the Life: I drive security initiatives and implement security controls that are in line with the business's security maturity program. This helps to provide assurance around the security of consumed IT services. I consider myself a technologist, and my knack for learning how things work keeps me very interested in cybersecurity to this day.

How I Got Started in Cybersecurity: In one of my previous jobs, I identified a gap: the need for better security practices. To solve for that gap, I focused on understanding the problem, then working on continuous learning, bite-sized cultural changes and implementations, and that's how I inadvertently launched my cybersecurity career. I enjoyed the discovery exercise of using appropriate security controls to mitigate risk, and then found that it was a valuable skill. I continued to learn, which reinforced my decision about my newfound career, and I never looked elsewhere.



My Advice: Learn wide early and specialize as you mature. Like a lot of professions, cybersecurity is wide-ranging, so a general exploration of the field early on can be a significant benefit as you begin your journey. Cybersecurity skills are more relevant now than ever. I have used a variety of resources to hone my cybersecurity skills. I read information security magazines, attend conferences, watch webinars, and follow technology trends like cloud, big data, and article intelligence, just to name a few.

Fun Fact: I spent a significant part of my upbringing in Nigeria.

Peter Ngo

Governance, Risk & Compliance Lead
Palo Alto Networks

Years in Cybersecurity: 15

"Be curious and be open to new things. If you want a steady job where you go in and do your eight hours, this may not be the right one. In cybersecurity, you are exposed to new things all the time. The hackers take plenty of time to perfect their craft, so you need to have the same diligence in learning about technology and how you can be safe and secure."

A Day in the Life: Within the Governance, Risk and Compliance team, I handle the compliance vertical, which includes external certifications, such as HIPPA (Health Insurance Portability and Accountability Act), SOC2 (Service Organization Control 2), and FedRAMP (Federal Risk and Authorization Management Program). I also lead third-party vendor risk assessments, especially if it's a SaaS (software as a service) product, and I help Sales with RFPs (requests for proposals) and RFIs (requests for information).

How I Got Started in Cybersecurity: My background is in accounting, and a I have a master's degree in IT auditing, but I've always had a passion for technology. I love learning about it and tinkering with it. I installed Windows when it was 3.1, the second Windows version that ever came out. I learned programming and developed a strong and broad technical background that continues to serve me well in cybersecurity. On top of the technology background, I have a strong interest in IT auditing, and a significant part of my training was validating systems controls, including electronic access and physical access. In one of my early jobs, I did IT audits of banks and tested them to see if they had the proper safeguards in place. I learned that often, the normal security procedures were not followed, and I was able to social engineer the bank staff to let me walk into parts of the bank that I was not authorized to be in and plug in USB devices. The gaps in security protocol can lead to huge risks for any organization.

My Advice: Be curious and be open to new things. If you want a steady job where you go in and do your eight hours, this may not be the right one. In cybersecurity, you are exposed to new things all the time. The hackers take plenty of time to perfect their craft, so you need to have the same diligence in learning about technology and how you can be safe and secure. Cybersecurity is so diverse. It goes from very technical to somewhat technical. If you're really technical, you can do threat hunting, security operations, engineering, or a range of other positions. Find out what your strong points are and then talk to the appropriate people working in cybersecurity to see what opportunities are available.

Fun Fact: I'm originally from Vietnam, but I came to the United States when I was young. After college, I had a chance to go back to Vietnam to work and spent 17 years of my career there. Cybersecurity is relevant around the world.

Ankur Jain

Senior Product Security Engineer
Palo Alto Networks

Years in Cybersecurity: 5

"My recommendation to anyone interested in the technical side of cybersecurity is to focus on honing your skills in operating systems, networking, and software development languages."

A Day in the Life: As a product security engineer, my mandate is to help teams employ secure development practices in the software development lifecycle. My team and I embed ourselves in the software development lifecycle, so we are involved and able to influence at each development phase of software development and deployment

How I Got Started in Cybersecurity: I became interested in security once I heard the term "cryptography" during my undergraduate studies. For a time, I thought, if we implement proper cryptographic code into our software, it will secure the product from any sort of attack, but I was quickly proven wrong during my internship where our mentor explained that, even if you have the most complex cryptographic implementation, there is nothing to stop a hacker from reverse engineering the code and bypassing the cryptographic control. This made me more curious, and my interest in researching in this area led me to where I am now. I completed my graduate studies in security engineering, but at the time there was not a strong job market in this field, so I initially started as a software engineer and tried to put myself in situations where I could work on development projects centering around security. I was fortunate that my first job was to implement a cryptographic feature. This gave me the confidence to push forward in asking for security-related projects later in my career.

My Advice: My recommendation to anyone interested in the technical side of cybersecurity is to focus on honing your skills in operating systems, networking, and software development languages. I would also suggest setting up your own test network. This hands-on experience will provide you with an environment to do security-based experimentation. Also, it's very helpful to become comfortable with at least one operating system. Security professionals love Linux because it is free and because the source code is available, which allows you to better understand the inner workings. Finally, I recommend learning programming languages, starting with a high-level or interpretative language. Python and Ruby are great starts to learn about native operating system functions. Alternatively, PHP and JavaScript provide a strong foundation in web-based technology. Once you have gained the confidence of building software applications, I would suggest trying to test them and working to find flaws that could be used for exploitation.

Fun Fact: I tend to quote famous lines from *Star Wars*, but I have yet to watch all of the movies.

Chris Honaker

Principal Product Security Architect
Palo Alto Networks

Years in Cybersecurity: 8+

"There are many different types of positions in cybersecurity. For some, learning tools is a great first step. For others, learning software engineering will help you with transitioning to software security."

A Day in the Life: I work on securing new product development throughout the software development lifecycle. This is done by integrating security into several touchpoints such as requirements, design, and implementation.

How I Got Started in Cybersecurity: I worked as a software engineer for several years and always had an interest in securing the software that I built. In my first job out of college, I was working at a school for real estate and financial services education. We were building a feature for our website that allowed students to register and pay for classes online. I was working on the back end, and the front-end developers asked me to test out some new features. In playing around with the site, I had found that I could inject JavaScript into one of the URL parameters, and by sending a link to someone, I could steal their session. At the time, I didn't know this was cross-site scripting (XSS wasn't really a thing then). My actual start in cybersecurity began when I worked as a product engineer for a company that built security products for the Department of Defense. In that same position, I started learning about cryptography, public key infrastructures, network security, and embedded engineering. I decided to get my master's degree from Virginia Tech and focus on information security.

My Advice: There are many different types of positions in cybersecurity. For some, learning tools is a great first step. For others, learning software engineering will help you with transitioning to software security. To keep up to date on current trends, articles and talks are good resources. I have an RSS feed that gives me a ton of both technical and non-technical articles around security. There is also a large cybersecurity community that you can take advantage of. There are several meetup groups and online groups where people chat and share information about all things security.

Fun Fact: Years ago, I wrote an entire implementation of Microsoft's Remote Desktop Protocol from scratch in C/C++.

Jake Smola

Red Team Intern
Palo Alto Networks

Years in Cybersecurity: 3

"Demonstrating the initiative to pursue cybersecurity projects and applying for cybersecurity-related work are two approaches that can yield high rewards in the near future."

A Day in the Life: I explored various security-related topics throughout my internship with the Red Team. I modeled and documented cyberattack techniques and procedures, automated attacks with Python and the popular Metasploit framework, and built a web application for interactive attack planning and tracking.

How I Got Interested in Cybersecurity: I became interested in cybersecurity during my undergraduate studies. I had been studying computer science at the United States Military Academy for about a year when I learned of the newly established Cyber branch of the Army. Before Cyber was revealed, relatively few Army positions involved the daily application of my academic discipline. My initial proclivity for cybersecurity thus arose out of convenience: working in the field would allow me to continue my professional development in computer science and ensure my skills could remain transferable to future civilian work. However, after learning about society's modern trend towards technological interdependence and its proportionate rise in cyberattacks, I realized the deeper significance of cybersecurity and fully committed myself to the field.

My Advice: Cybersecurity is a large, diverse field, relevant to just about any digital device or service. To learn about cybersecurity, I highly recommend exploring some publicly available resources, including news reports, blog posts, and conference proceedings, covering cyberattacks or vulnerabilities and the technologies they affect. From this preliminary investigation, I would choose one or two technologies (web applications, computer networks, cipher suites, etc.) that are interesting and focus your follow-on learning on these technologies. Follow-on learning could begin with security courses or other professional tutorials that offer a thorough exploration of the technology or topic without requiring many prerequisites. Next, I would revisit some of the initial resources gathered, as well as other papers and blog posts, to apply what I learned in the coursework and gain a deeper understanding. Finally, I would pursue hands-on, technical experiences with security-related applications. This could include participating in capture the flag events, developing secure software, or otherwise challenging yourself with a deeper exploration of a complex system. The demand for security professionals is ever-increasing. Demonstrating the initiative to pursue cybersecurity projects and applying for cybersecurity-related work are two approaches that can yield high rewards in the near future.

Fun Fact: I grew up in Prague.

Ashley Richardson

Security Training Engineer
Palo Alto Networks

Years in Cybersecurity: 2

"When I was born, it was the onset of personal computers. I found computers to be incredibly interesting. I loved gaming, and I was really into reading manuals for debugging phones and early software."

A Day in the Life: I am responsible for post-sales training to our customers and conduct a monthly internal product training for my coworkers. I normally fly out on Sunday morning to an on-site location, teach for the week and fly home on Friday. Right now, I'm mostly teaching our Firewall Essentials Class. On occasion, I get to volunteer with youth interested in technology and enjoy speaking at conferences. When I'm not on the road, I'm working on my own firewall, keeping up to date with the latest cybersecurity news and threats, and studying for additional certification.

How I Got Started in Cybersecurity: When I was born, it was the onset of personal computers. I found computers to be incredibly interesting. I loved gaming, and I was really into reading manuals for debugging phones and early software. Then I saw the movie Hackers, and I was sold. Later, when I was in the military, I took a class for my Security+ certification, and I never looked back.

My Advice: It took me a while to get the opportunity to actually work in cybersecurity. My advice is to ask a lot of questions, go to events, network and keep in touch with the people you meet. I found a mentor at my last job, and he is the one who told me about Palo Alto Networks VetsinTech class. It was because of that class that I eventually was hired to work at a cybersecurity company.

Fun Fact: I really like comics and video games. I used to play Dance Dance Revolution religiously.

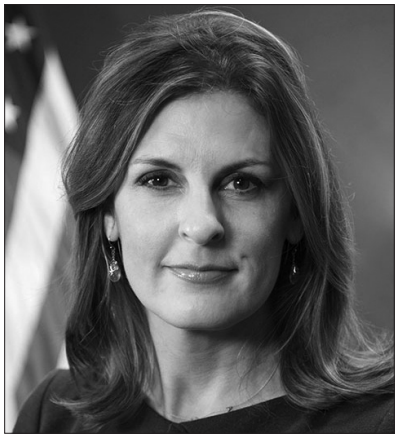
Chapter 6:
Be a Lifelong Learner

Erin Nealy Cox

U.S. Attorney for the Northern District of Texas
Department of Justice

Years in Cybersecurity: 17

"Keep an open mind about your career path and take on new opportunities that may lead you in new directions. A non-traditional opportunity may come to you and it could take you down a road you never considered—but one that opens up a whole new world of possibilities."



A Day in the Life: As U.S. Attorney for the Northern District of Texas, I am the chief federal law enforcement officer responsible for all federal criminal prosecutions and civil litigation involving the United States in the Northern District of Texas, which covers 100 counties, over 96,000 square miles, and a population of approximately eight million. I oversee a staff of approximately 115 attorneys and a similar number of non-attorney support personnel assigned among five division offices. Now that I'm going back into law from the world of cybersecurity consulting, I have a strong understanding of how cyber touches everything we do. Instead of identifying something as "cyber crime" as we have done in the past, we need to start thinking about all crime as just crime—most of which is facilitated by cyber in one way or another.

How I Got Started in Cybersecurity: I was a federal prosecutor when the 9/11 attacks happened in 2001. I wanted to help and serve my country in whatever way I could, so when the Department of Justice (DOJ) added a number of resources to cyber, I was asked to start working in the cyber section. This section was formalized, given the nexus between cyber and counterterrorism and anti-terrorism investigations. The cybersecurity field fascinated me, especially when working on investigations where I learned to track the digital evidence and really dig into a deeper understanding of how the attackers got in, and how they were getting data out. I'm trained in law, not code, but I worked with many brilliant professionals who helped me to understand the intricacies of cyber crimes so I could explain the findings to others who did not have a technical background but needed to make very important business decisions. Before my appointment as U.S. Attorney, I worked as a Senior Advisor at McKinsey & Co. in their Cybersecurity and Risk practice. Prior to that, I was a member of the executive leadership team at Stroz Friedberg, a cybersecurity and investigations consulting firm, ultimately leading the firm's global Incident Response Business.

My Advice: If you didn't study engineering or computer science, but you're interested in learning about enterprise liability and cyber risk, you can use your knowledge and skills from other disciplines. Keep an open mind about your career path and take on new opportunities that may lead you in new directions. A non-traditional opportunity may come to you, and it could take you

down a road you never considered—but one that opens up a whole new world of possibilities. I'm also passionate about encouraging women and kids to try out different paths and learn as much as you can because cybersecurity needs you. I have three daughters, and there's a lot that parents and kids can do to be safer online. Nowadays, the news highlights on a daily basis talk of cyber crime. We can use this awareness to our advantage to protect ourselves and our data.

Fun Fact: I am a member of both the Texas and New York bar associations. I received my Juris Doctor degree, magna cum laude, from Southern Methodist University Dedman School of Law and my Bachelor of Business Administration in finance from the McCombs School of Business at the University of Texas at Austin.

Stan Lee

Director, Security Architecture
Palo Alto Networks

Years in Cybersecurity: 20

"My advice to those who may be just starting out in cybersecurity is to learn as much as you can from anywhere and anyone."

A Day in the Life: I lead the security architecture team, which has two primary responsibilities. First, my team defines the strategic security capabilities and services for Palo Alto Networks, which addresses the business risks and requirements of the company. Second, my team is responsible for product security, which ensures our products and customer-facing services are designed, developed, and deployed securely.

How I Got Started in Cybersecurity: I became interested in this field because I've always been a perpetual learner—a self-described lifelong learner. Early in my career, I had the fortunate opportunity to be exposed to cybersecurity and realized that it is also the only technology domain that spans everything, including hardware, software, infrastructure, network, data center, public hosting, and more. When I was working part-time while pursuing my bachelor's degree, I was part of the team that deployed the first switched Ethernet-connected student housing in the University of California system. It was truly the wild west from the perspective of network infrastructure and security. I had the opportunity to work with the network and infrastructure manager, who showed me how to deploy the first enterprise stateful firewall then.

My Advice: I have been working in cybersecurity for more than 20 years in multiple roles. I have also worked in multiple industry verticals, including in the public and private sectors. My advice to those who may be just starting out is to learn as much as you can from anywhere and anyone. There is a tremendous amount of content available now. There are formal training and certification programs, which are always a good way to discover what each area entails. In addition, there is open source content available, which includes technical and domain-specific material. I definitely recommend spending time and truly understanding the foundation, and you may be surprised how much more interesting it becomes at that level. Cybersecurity really does have a broad scope, and you can build a career on what motivates you the most. If you are passionate about technologies, start implementing them to understand how they work. If you are interested in the business side, then learn about risk assessment and how to balance risks and benefits. If you are passionate about education, network with other cybersecurity professionals and understand their experience.

Fun Fact: I have a bachelor's degree in biochemistry and started my career in cancer research. My background in research and the scientific approach extends well into cybersecurity, and it is something that I still get to apply on a daily basis.

Archana Muralidharan

Solution Architect, Governance, Risk & Compliance
Palo Alto Networks

Years in Cybersecurity: 9

"Cybersecurity is all about confidence. Having a strong engineering technology base can help you to be a strong cybersecurity professional. Try your hands at developing code. Work as an application developer or a network engineer before switching to security so that you know the technology landscape and you have a deep and clear understanding of how things work."

A Day in the Life: In my current job, I am responsible for implementing information security controls. I work closely with various teams like Engineering, Architecture and the SOC from a compliance perspective. I also work with different stakeholders outside of information security, including in product management and IT to roll out security-related controls for the organization.

How I Got Started in Cybersecurity: Initially, I didn't know much about cybersecurity. I worked as a developer for close to five years, and then I started working at a new company where I learned that I was coding in an insecure way. When I started working in applications security and understanding secure coding practices, I looked back and realized that what I had developed could have been improved from a security perspective, which was thrilling to learn. My career shift into the Governance, Risk and Compliance function happened organically. I worked for the Department of Human Services in Washington, D.C., under President Obama. We implemented security solutions to make sure we were in compliance.

My Advice: Cybersecurity is all about confidence. Having a strong engineering technology base can help you to be a strong cybersecurity professional. Try your hands at developing code. Work as an application developer or a network engineer before switching to security so that you know the technology landscape and you have a deep and clear understanding of how things work. If you are making a career change like I did, you can find tutorials on how to program so you can speak the language of a developer. If you have a real zeal to work in cybersecurity, there is so much opportunity. There are so many free resources online these days to become more familiar and get your feet wet. Then you can look at getting a degree or certification.

Fun Fact: I love singing. It truly gives me joy and peace.

Vasu Kohli

Senior Director of Governance, Risk & Compliance
Palo Alto Networks

Years in Cybersecurity: 20

"Cybersecurity is not a nice, well-planned-out, and scenic car ride. It's more of a windy road with a ton of potholes, and you're driving without a seatbelt at high speeds."

A Day in the Life: My primary responsibilities are to design and implement sustainable information security governance, risk-management, and compliance programs for the company. The heart of the GRC function is understanding the business, regulatory, and competitive landscapes and translating those back to the organization in the form of operating requirements. The world of GRC is a very externally focused. Risk management is the heart of the GRC function because it is a decision-making system. Governance is more of a management interface, and compliance is more of an external interface. At a high level, risk management is really the engine of the car that makes everything work.

How I Got Started in Cybersecurity: I got introduced to the cybersecurity industry from a technologist's perspective. I started out building desktops; then wiring walls, closets, and ceilings; and then worked my way up into learning how to configure servers. I started on the ground floor, and then got a lot of exposure to multiple focus areas and decided that GRC was a natural fit for me. I have found that GRC was the way to clearly articulate and measure concerns I had about that technology environment. That got me more into security assessment and then risk assessment. Then, I started to understand compliance and the role that it plays in a risk-management decision-making system and governance. From a personal standpoint,

GRC allows you to exercise a lot of creativity in the way you articulate your compliance posture and provide value to the environment. It takes a lot of relationship management skills, and those are challenges I enjoy working on.

My Advice: Stay passionate about learning. Don't worry about not knowing everything. This is a field that is constantly evolving. You have an awesome opportunity to be at the very start of a profession that is in its formative years. Don't stop learning, but do not get overwhelmed with the amount of learning. Cybersecurity is not a nice, well-planned-out, and scenic car ride. It's more of a windy road with a ton of potholes, and you're driving without a seatbelt at high speeds. If you like operating in that sense of chaos, continue to learn and be one of the first to explore the road ahead.

Fun Fact: As responsible and risk-minded as I am at work, I am equally playful at home, particularly with my kids. There is a balance in life, and I try to live on both sides of the equation.

Anshul Arora

Infrastructure Security Architect
Palo Alto Networks

Years in Cybersecurity: 10

"Never fear asking questions because that's when you learn the most. Asking questions gives you an opportunity to connect with people and lets you have a deeper understanding of the topic."

A Day in the Life: In my current role, I am an Infrastructure Security Architect with responsibility for securing our organization's infrastructure—including routers, switches, servers, firewalls, and more—to prevent unauthorized access to our company's data and resources. This is for both on-premises and public cloud data centers.

How I Got Started in Cybersecurity: I started as a network security engineer and then moved to cybersecurity. On one of my early cybersecurity projects, I was part of a QA team testing the security appliance features. Since that initial experience, my interest in this budding field has increased tenfold.

My Advice: One way to begin learning about cybersecurity is to just start exploring the web. Then, put into practice what you've learned. Cybersecurity is such a vast field, where you'll find something that's really interesting to you, and then you can decide to go deeper into learning more about that particular topic. The more time you spend learning, the more you'll excel. Also, make it a point to structure your learning by taking a certification exam to mark major milestones on your journey to mastering specific topics in cybersecurity. Finally, never fear asking questions because that's when you learn the most. Asking questions gives you an opportunity to connect with people and lets you have a deeper understanding of the topic. I enjoy sharing knowledge on cybersecurity-related topics with colleagues at work and also the broader cybersecurity community.

Fun Fact: I feel refreshed when I can spend time outdoors with my family, either stargazing or going beyond the trails.

Ron Dodge

Senior Director, Security Engineering
Palo Alto Networks

Years in Cybersecurity: 16

"Have a passion for understanding how things work. If you don't have passion for what you do, number one, you won't like it; and two, you won't be good at it."

A Day in the Life: Security engineering is a vital function in ensuring that cybersecurity solutions and functionality are appropriately planned and executed in support of business goals. I partner with other security verticals, as well as our business partners, on bringing security solutions to the business to support the requirements identified.

How I Got Started in Cybersecurity: I really got interested in technology when I built a video game as an undergraduate student. It was a really mundane video game. Even though it wasn't very robust or good visually—just using lots of 0s and brackets—building a game that actually did something was pretty cool. I have my undergraduate, master's, and Ph.D. in computer science; but I first got into cybersecurity in 2002 when I was appointed to be a senior research scientist in a research center that had been focused on artificial intelligence. Later in that role, I started looking at defending and securing our systems from malicious intent and building things in a secure manner, and that's how I got started in cybersecurity.

My Advice: Have a passion for understanding how things work. As a security architect, security engineer, or security operations analyst, it helps to understand why something is happening and how it's supposed to work. To improve in your career, you need to know what you don't know. If you are not upfront about where you need outside expertise, credibility gets lost very quickly.

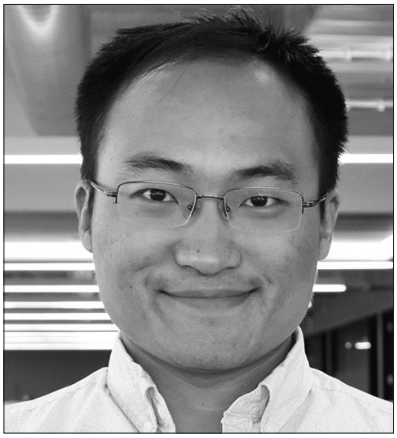
Fun Fact: I love the outdoors; I am just as happy pulling weeds as creating a project plan.

Jason Chen

Information Security Data Engineer
Palo Alto Networks

Years in Cybersecurity: 1

"Like a joke our CISO told us, we are the 'bodyguard for The Rock' because we work on the information security team for a cybersecurity company. I like the excitement of the role. I think it is amazing when your skills meet your interests."



A Day in the Life: I work to facilitate security operations and analysis with the help of data science. On one hand, I build data pipelines to collect massive amounts of security log data and process them for the downstream security analysis. On the other hand, I leverage machine learning algorithms to detect anomalies in the logged data.

How I Got Started in Cybersecurity: While I was completing my Ph.D., I got an internship to work on a cybersecurity team. Fortunately, the data science skills I learned in school could be leveraged in a security domain. Before I graduated, I was offered a full-time position, and I accepted. Like a joke our CISO told us, we are the "bodyguard for The Rock" because we work on the information security team for a cybersecurity company. I like the excitement of the role. I think it is amazing when your skills meet your interests.

My Advice: Since I'm just entering this field, I know firsthand what it's like to be required to learn many new things. I would suggest taking advantage of online resources. Also, find activities like cybersecurity hackathons or capture the flag events for hands-on security experience, meet with experienced practitioners to learn best practices from them, and go to conferences for exposure to cutting-edge technology. In many ways, cybersecurity is fundamental to modern life. The more hacks happen, the more I realize how important cybersecurity is. It's hard to imagine a world without the police to protect us. Similarly, in the digital world, it's hard to imagine living without cybersecurity professionals, tools, and processes to protect us and our information.

Fun Fact: When I was young, I was left-handed but later changed to be right-handed. You can find me using scissors with my left hand, while I eat and write with my right hand.

Arkadiusz Kotowski

Cybersecurity Academy Manager, International
Palo Alto Networks

Years in Cybersecurity: 3

"It's been three years since I started my new adventure in cybersecurity, and this has become more than just my work—it is now my lifestyle."

A Day in the Life: It's not an exaggeration when I say that every day looks entirely different. I lead the Cybersecurity Academy program, focusing on Europe, the Middle East, Africa, and Asia. Our mission is to protect life in the digital age one student at a time. To bridge the cybersecurity skills gap, I collaborate not only with the educational institutions but also with our partners, customers and, most importantly, my colleagues from all over the world. My daily tasks include recruiting and onboarding new academic partners, and organizing events and competitions, raising the awareness of the program and cybersecurity either remotely or by visiting our customers and partners onsite.

How I Got Started in Cybersecurity: When I was growing up, I never considered working in cybersecurity. It was pure coincidence, and it turned out to be the best career choice I've ever made. One of my friends who happened to be a Palo Alto Networks system engineer referred me for a business development role. It's been three years since I started my new adventure in cybersecurity, and this has become more than just my work—it is now my lifestyle.

My Advice: I believe there are a lot of stereotypes and myths about cybersecurity. Some say cybersecurity professionals are "nerds" or "geeks." Actually, it is quite the opposite. People in this industry are some of the coolest people you will ever work with. Also, not many people are aware that specific skills are transferable to cybersecurity: communication and leadership, problem-solving, analytical thinking, and business risk experience, to name a few. I've learned that there is room in the cybersecurity industry for everyone who is willing to stay open to change and learn new skills on the go. A career in cybersecurity is like riding a roller coaster—it's super exciting and very gratifying. My advice is never take anything for granted and feel empowered to test out your entrepreneurial and creative skills. Ask yourself questions such as, "Is my work adding value?" and "How can I help others achieve their goals?" To be successful, focus on the big picture and remember that this is a team sport. We are on this journey together.

Fun Fact: I lived and worked in five different countries in the past 15 years. I am originally from Poland. I have lived and worked in Ireland, United Kingdom, Australia, Netherlands, and Poland. I met my wife in Ireland. My daughter was born in Amsterdam.

Chapter 7: Recommended Resources

Recommended Resources

"Confidence comes from preparation. When you don't know about a subject matter, learn about it. The more you learn, the less scary it will seem." –Elias (Lou) Manousos, CEO, RiskIQ

Continuous learning is required to be successful in cybersecurity. Many of the cybersecurity professionals featured in this guide shared the resources they use regularly to learn in their work. What follows are a few such resources to help you build your knowledge as you begin your journey in cybersecurity.

Websites

This is just a sample of the many excellent sites on cybersecurity out there:

- **Bleeping Computer®** [www.bleepingcomputer.com]: In this free community, 700,000+ registered members discuss and learn how to use their computers.
- **CIS Critical Security Controls** [www.cisecurity.org/controls/]: The Center for Internet Security (CIS) is a nonprofit organization that puts out global standards and best practices for Internet security—for securing IT systems and data against attacks.
- **Cybersecurity Canon** [cybercanon.paloaltonetworks.com]: Hosted by Palo Alto Networks, this site lists must-read books for all cybersecurity practitioners—be they from industry, government, or academia—where the content is timeless, genuinely represents an aspect of the community that is true and precise, reflects the highest quality, and if not read, will leave a hole in the cybersecurity professional's education that will make the practitioner incomplete.
- **The Cyber Security Place** [www.thecybersecurityplace.com]: This site is dedicated to collecting and disseminating pertinent cybersecurity matters threatening financial and business operations of companies around the globe.
- **The CyberWire** [www.thecyberwire.com]: A community-driven cybersecurity news service, CyberWire provides concise briefings on the critical news happening across the global cybersecurity domain.
- **How-To Geek®** [www.howtogeek.com]: This online tech publisher is dedicated to explaining the "hows" and the "whys" of technology news.
- **HackerRank®** [www.hackerrank.com]: Working to match developers to the right job, HackerRank provides a technical recruiting platform that assesses developers based on coding skills.
- **Dark Reading®** [www.darkreading.com]: Within this widely read cybersecurity news site and online community for security professionals, learn about new cyberthreats, vulnerabilities, and technology trends.
- **InfoSec Conferences** [infosec-conferences.com]: The cybersecurity community utilizes this resource to find information about cybersecurity conferences taking place around the world.
- **IT Security** [www.itsecurity.co.uk]: Run by a small, independent organization, the goal of this site is to discuss information security in a new and challenging manner.

- **IT Security Guru** [www.itsecurityguru.org]: Get a daily news digest of all the top breaking IT security news stories here each morning.
- **Open Security Training** [www.opensecuritytraining.info]: This site conveys security information in the form of structured instructor-led classes.
- **Over the Wire** [www.overthewire.org]: Learn and practice security concepts in the form of fun-filled games.
- **Reddit®** [www.reddit.com]: Check out the security and programming subreddits.
- **SANS Institute** [www.sans.org]: SANS is one of the largest sources for information security training and security certification in the world. It also develops, maintains, and makes available—at no cost—research documents about various aspects of information security.
- **Security Roundtable** [www.securityroundtable.org]: Powered by Palo Alto Networks, this is a one-stop resource for business leaders looking for insightful, actionable information about cybersecurity best practices. If you're just getting started, this is a good resource to see what cybersecurity leaders and experts are thinking and talking about.
- **Security Through Education** [www.social-engineer.org]: Information found here is designed to help corporations learn how to combat and mitigate the effects of malicious social engineering.
- **Security Weekly** [www.securityweekly.com]: A podcast network and accompanying newsletter, Security Weekly provides content within the subject matter of IT security news, vulnerabilities, hacking, and research.
- **Slashdot®** [www.slashdot.org]: This is a source for technology-related news with a heavy slant toward Linux and open source issues.
- **Tech Exams** [www.techexams.net]: Access free online practice exams here as well as active forums and links to free resources for Microsoft® MCSA, MCSE, MCTS, and MCITP; Cisco® CCNA, CCDA, and CCNP; CompTIA A+, Network+, and Security+; and InfoSec certifications, such as CEH and CISSP.
- **Threat Level** [www.wired.com/category/threatlevel]: This is the cybersecurity section of Wired magazine.
- **Threat Post** [www.threatpost.com]: An independent news site, Threat Post is a leading source of information about IT and business security for thousands of professionals worldwide.
- **Twitter®** [www.twitter.com]: Follow prominent members of the information security community.
- **VulnHub** [www.vulnhub.com]: Access materials allowing anyone to gain practical, hands-on experience in digital security, computer software, and network administration.
- **Woman In Cyber** [woman-in-cyber.com]: This website offers resources encouraging women in cybersecurity to expand their potential and grow in their careers.

Blogs

Blogs can be very helpful resources for cybersecurity practitioners because they offer analysis and perspectives from experts in the industry. Here are just a few examples:

- **Schneier on Security** [www.schneier.com]: Bruce Schneier is an internationally renowned security technologist, and author of 13 books—including Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World—as well as hundreds of articles, essays, and academic papers.
- **Krebs on Security** [www.krebsonsecurity.com]: Brian Krebs worked as a reporter for The Washington Post from 1995 to 2009 and is the author of Spam Nation: The Inside Story of Global Cybercrime.
- **Elie Bursztein Blog** [elie.net/blog]: Bursztein blogs about web technologies and games with a focus on performance and security.
- **Graham Cluley** [grahamcluley.com]: Cluley is an independent computer security analyst and has worked in the computer security industry since the early 1990s.
- **Emergent Chaos** [emergentchaos.com]: This is a group blog on security, privacy, liberty, and economics.

Organizations and Associations

Once you learn more about cybersecurity, familiarize yourself with key organizations and associations in the industry to access resources and interact with experts and fellow practitioners. These include:

- **ISACA** [isaca.org]: ISACA is a nonprofit, independent association that advocates for professionals involved in information security, assurance, risk management, and governance.
- **(ISC)²** [isc2.org]: The International System Security Certification Consortium is an international, nonprofit membership association for information security leaders, including over 130,000 certified members. The organization provides globally recognized certifications, networking and collaboration opportunities, and development and leadership tools.
- **OWASP** [owasp.org]: The Open Web Application Security Project is a global nonprofit organization focused on improving the security of software.
- **CSA** [cloudsecurityalliance.org]: The Cloud Security Alliance is dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment.

Certifications

Getting certified can help you gain a deeper understanding in certain areas. Certifications include:

- CCSK – Certificate of Cloud Security Knowledge
- CEH – Certified Ethical Hacker

- CGEIT – Certified in the Governance of Enterprise IT
- CIPP – Certified Information Privacy Professional
- CISA – Certified Information Systems Auditor
- CISM – Certified Information Security Manager
- CISSP – Certified Information Systems Security Professional
- CRISC – Certified in Risk and Information Systems Control
- GIAC – Global Information Assurance Certification
- ISSMP – Information Security System Management Professional
- TPECS – Training Provider and Examiner Certification Scheme

Resources for Kids

Kids can use these resources to learn more about technology and how to be safe and secure online:

- Codecademy® [www.codecademy.com]
- CyberPatriot [www.uscyberpatriot.org]
- Khan Academy® [www.khanacademy.org]
- Kids in Cybersecurity Hub [go.paloaltonetworks.com/ghzuky]
- PRIVO [www.privo.com]
- SANS Cyber Aces [www.cyberaces.org]
- SANS CyberStart [www.sans.org/cyberstart]
- The Tech Challenge [www.thetech.org/thetechchallenge]
- U.S. Cyber Challenge [www.uscyberchallenge.org]

Cybersecurity Career Guide

Cybersecurity needs you. Beginning a new career path in cybersecurity can be daunting, especially if you don't know what to do, who to talk to, and whether you're even ready to get started. The goal for this book is to provide the information you need to kick-start your career in cybersecurity. We reached out to some of the best cybersecurity practitioners in the industry and asked them to share their insights. How did they get started? What resources did they use to learn? What major factors helped advance their knowledge and expertise in cybersecurity? You will learn all of this—and more—here.

By 2021, there will be 3.5 million unfilled cybersecurity jobs. The next generation of cybersecurity professionals needs to have diverse skills, experiences, and mindsets. You can be part of the digital ecosystem, where you have a unique opportunity to be a thought leader and shape the future of cybersecurity. Will you join us?