How to build a successful career in cybersecurity

TechRepublic

How to build a successful career in cybersecurity

Published by TechRepublic

August 2017

Disclaimer

The information contained herein has been obtained from sources believed to be reliable. CBS Interactive Inc. disclaims all warranties as to the accuracy, completeness, or adequacy of such information. CBS Interactive Inc. shall have no liability for errors, omissions, or inadequacies in the information contained herein or for the interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

TechRepublic

9920 Corporate Campus Dr.

Suite 1000

Louisville, KY 40223

Online Customer Support:

http://techrepublic.custhelp.com/

CREDITS

Global Editor in Chief
Jason Hiner

Editor in Chief, UK
Steve Ranger

Managing Editor
Bill Detwiler

Editor, Australia
Chris Duckett

Senior Features Editors
Jody Gilbert
Mary Weilage

Senior Editor
Conner Forrest

Senior Writers
Dan Patterson
Teena Maddox

Chief Reporter
Nick Heath

Staff Writers
Hope Reese
Alison DeNisco
Brandon Vigliarolo

Associate Editor
Amy Talbott

Multimedia Producer/Editor
Derek Poore

Associate Social Media Editor
Leah Brown

Cover image: iStock/ FroYo_92

Contents

Want a career in cybersecurity? Here are 10 jobs to explore

By Alison DeNisco

With a growing cyber threat landscape and an estimated 1 million unfilled cybersecurity jobs worldwide, the field is wide open for both recent graduates and people looking to make a career change.

Job postings in the cybersecurity field have gone up 74% over the past five years—and US News and World Report ranked a career in information security analysis fifth on its list of best technology jobs. Average salaries nationally are $88,890, and significantly higher in cities such as San Francisco and New York

"The job prospects are excellent," Deborah Hurley, a professor for Brown University's executive master in cybersecurity program, told TechRepublic recently. "The demand far outstrips the supply."

Here are 10 job options to explore in the cybersecurity field, with job description information from CyberDegrees.org.

1. Security consultant

"A security consultant is the IT equivalent of Obi-Wan—advisor, guide, and all-round security guru," according to CyberDegrees.org. People in this role design and implement the strongest possible security solutions based on the needs and threats facing an individual company, and day-to-day tasks may vary widely. A security consultant might determine the most effective way to protect computers, networks, software, data, and information systems against attacks, perform vulnerability testing and risk analyses, test security solutions, respond to any incidents, and update security systems as needed, depending on the terms of their contract.

2. Chief information security officer

The chief information security officer (CISO) is the leader of all security initiatives in a company. While these tech professionals were traditionally seen as security enforcers, they are now often considered strategists, helping the enterprise avoid cybercrime. CISOs typically appoint and guide a team of security experts, create a strategic plan for the deployment of information security technologies and programs, develop corporate security policies, and monitor security vulnerabilities, among a number of other tasks.

3. Security engineer

Security engineers are intermediate-level employees who build and maintain IT security solutions for a company. These professionals develop security for the organization's systems and projects and handle any technical problems that arise. Security engineers are often responsible for configuring and installing firewalls and intrusion detection systems, performing vulnerability testing, developing automation scripts to track incidents, and testing security solutions.

4. Security architect

The senior-level security architect position involves designing, building, and overseeing the implementation of network and computer security for a company. Security architects must plan, research, and design strong security architectures for all IT projects, perform security assessments, respond to incidents, develop requirements for LANs, WANs, VPNs, routers, firewalls, and other network devices, and design PKIs, among other tasks.

5. Incident responder

An incident responder (sometimes called a computer security incident response team engineer or an intrusion analyst) is essentially a cyber firefighter and must rapidly address security threats and incidents within a company. "In your role as a first responder, you will be using a host of forensics tools to find the root cause of a problem, limit the damage, and see that it never happens again," according to CyberDegrees.org. "Like a firefighter, part of your job will also involve education and prevention." This involves actively monitoring systems and networks for attacks, identifying security vulnerabilities, performing malware analysis and reverse engineering, and establishing protocols for communication within an organization and with law enforcement during a security incident.

6. Computer forensics expert

A computer forensics expert acts as a digital detective, accessing and analyzing evidence from computers, networks, and data storage devices. On a day-to-day basis, this role involves conducting security incident investigations, recovering and examining data from devices, compiling evidence for legal cases, and advising law enforcement on the credibility of acquired data. These experts often work for large corporations, law enforcement agencies, legal firms, private consulting firms, and the government.

7. Penetration tester

Penetration testers, also know as ethical hackers, are responsible for legally hacking into an organization's applications, networks, and systems to discover and later patch security vulnerabilities. This role involves creating and performing formal penetration tests, conducting physical security assessments of servers, systems, and network devices, using social engineering to discover security flaws, and incorporating business considerations into security strategies.

8. Security analyst

A security analyst detects and prevents cyber threats for a company. This might involve planning, implementing, and upgrading security measures and controls, performing risk analyses, conducting internal and external security audits, managing network, intrusion detection, and prevention systems, and coordinating security plans with third-party vendors.

9. Security software developer

These tech professionals develop security software and integrate security into applications software during the design and development process. Depending on the specific position and company, a security software developer might oversee a team of developers in the creation of secure software tools, develop a company-wide software security strategy, participate in the lifecycle development of software systems, support software deployments to customers, and test their work for vulnerabilities.

10. Security auditor

A security auditor is a mid-level role that entails examining the safety and effectiveness of company computer systems and their security components and then issuing a detailed report outlining the success of the system and any changes or improvements that could be made. These professionals plan, execute, and lead security audits across a company, evaluate the efficiency, effectiveness, and compliance of operational processes with corporate security policies and any government regulations, and develop and administer risk-focused exams for IT systems.

10 programs to help you break into a cybersecurity career

By Alison DeNisco

Some 82% of IT professionals report a shortage of cybersecurity skills in their business, according to a 2016 survey from Intel—and 71% cited this shortage as responsible for direct and measurable damage to organizations whose lack of talent makes them easier hacking targets.

Job postings in the cybersecurity field have gone up 74% over the past five years. And US News and World Report ranked a career in information security analysis fifth on its list of best technology jobs. Average salaries nationally are $88,890 and significantly higher in cities such as San Francisco and New York.

Interested in a career in cybersecurity? Here are 10 programs for earning bachelor's and master's degrees and certifications that can help you get started at any education level.

1. Drexel University

BS in Computing and Security Technology

Drexel University's BS in Computing and Security Technology consistently tops lists of cybersecurity preparation programs and is recognized as a National Center of Academic Excellence in Information Assurance Education by the NSA. It offers hands-on experience managing and operating computer servers, networks, web and mobile systems, and databases, with a focus on security. Students can enroll in either the full-time, on-campus degree program or in the online, part-time degree completion program, targeted at people who have already earned an associate's degree.

2. University of Maryland University College

BS in Computer Networks and Cybersecurity, BS in Cybersecurity Management and Policy, BS in Software Development and Security

University of Maryland University College offers three bachelor's, four master's, and four certificate programs focused on different aspects of cybersecurity. The school is designated as a National Center of Academic Excellence in Cyber Defense Education by the NSA and is headquartered between the DoD's Cyber Command in Maryland and the Cyber Corridor in Virginia. The UMUC Cyber Padawans cybersecurity competition team took home the first place prize in last year's Cyber DiploHack event.

3. Pennsylvania State University

BS in Security and Risk Analysis-Information and Cyber Security

Penn State's BS in Security and Risk Analysis degree, named one of the top online bachelor's programs by US News & World Report, focuses on the technologies, education, and policies needed to protect people

and information. Students learn to design secure systems, evaluate and measure risk, and ensure privacy maintenance for individual users, businesses, and governments. Penn State is also recognized as an NSA Center of Academic Excellence in Cyber Defense. The program is available online.

4. University of Denver

MS in Cybersecurity

The University of Denver's MS in Cybersecurity program immerses students in the field, allowing them to work with local industry partners on real-world problems. The one-year, fast-track master's degree comes with a discounted scholarship of nearly 50% and does not require students to have an undergraduate degree in computer science. University of Denver's program is also designated as an NSA Center of Academic Excellence in Cyber Defense.

5. Champlain College

BS in Cybersecurity, MS in Digital Forensic Science, Cybersecurity Certificate

Champlain College offers online bachelor's and master's degrees and certificate programs in cybersecurity designed for working adults. It is the two-time winner of SC Magazine's Best Cybersecurity Higher Education award and is designated as an NSA National Center of Academic Excellence in Cyber Defense. The curriculum is career-focused and provides strategic thinking skills and solution sets applicable to the workforce.

6. Illinois Institute of Technology

MS in Cyber Forensics and Security

Illinois Institute of Technology offers several security-oriented programs at the undergraduate, graduate, and certificate levels. The Master's of Cyber Forensics and Security program is unique in that while students take cybersecurity courses, they also take legal courses alongside law students of the Illinois Institute of Technology Chicago-Kent College of Law. The program is designed to help students and experienced IT professionals become cybersecurity managers. The school is also designated as an NSA National Center of Academic Excellence in Cyber Defense.

7. EC-Council Certified Ethical Hacker certification

The International Council of E-Commerce Consultants (EC-Council) is the world's largest cybersecurity technical certification organization. Its Certified Ethical Hacker certification involves a training course that teaches students to look for weaknesses and vulnerabilities in a system using the same tools as a malicious hacker but in a lawful way to assess the security systems. It is a vendor-neutral certification. Those who want to take the certification exam without training must demonstrate two years of information security experience.

8. CompTIA Security+ certification

With more than 250,000 credential holders, CompTIA Security+ is a popular, vendor-neutral security certification with an available online learning tool for preparation. Exam content stems from a combination of industry-wide survey feedback and contributions from a team of security experts. The certification is approved by the US Department of Defense to fulfill cybersecurity position requirements and is compliant with government regulations under the Federal Information Security Management Act. Companies that recognize the certification include Apple, Dell, HP, IBM, and Intel.

9. GIAC Security Essentials Certification (GSEC)

The GIAC Security Essentials Certification (GSEC) is intended for security professionals who want to demonstrate that they are qualified for IT systems hands-on roles in terms of security tasks. Credential holders will demonstrate knowledge and technical skills in areas including network mapping, access controls, password management, and cryptography fundamentals. No specific training is required, but CIAC recommends a boot-camp style preparation course from SANS.

10. International Information Systems Security Certification Consortium Certified Information Systems Security Professional certification

The Certified Information Systems Security Professional (CISSP) is an advanced-level, vendor-neutral certification for IT professionals looking to expand their career into information security. The certification is meant to prove credibility in designing, implementing, and managing overall information security programs to protect organizations from sophisticated attacks. In-person and online training programs are available through (ISC)2 and third-party companies. Interested individuals must have a minimum of five years of full-time work experience in two or more of the eight domains listed here.

The 3 most in-demand cybersecurity jobs of 2017

By Alison DeNisco

Cybersecurity roles rank among the most difficult to fill in the enterprise, with the talent gap in this field expected to reach 1.8 million jobs by 2022. This is a major problem, as threats such as ransomware are at an all-time high, according to Stephen Zafarino, senior director of recruiting at Mondo, a national staffing agency specializing in niche IT, tech, and digital marketing talent.

"It definitely can be a challenge—demand is extremely high, and supply is very low, so it's a candidate's market," Zafarino said. "Companies see the benefit of making sure they are investing in the right talent from the best places and are definitely paying a heavy price as a result."

The average salary for a cybersecurity engineer is between $110,000 and $160,000, Zafarino said. And skilled candidates are more able to negotiate salary, benefits, and perks such as working remotely than in the past, he added.

Here are the three most in-demand cybersecurity jobs this year, according to Mondo.

1. Penetration testers

Ransomware is on the rise. After the Petya attack, Zafarino said he received "plenty of phone calls about how to achieve higher security, and who can come evaluate it." Penetration testers are often a good way to do that, as they go into your system and find vulnerabilities. From there, they will either correct the issue or offer a detailed report of the flaws in the system so a company can bring in cybersecurity engineers or analysts to fix them and make sure no outside source can break in.

2. Cybersecurity engineers

Cybersecurity engineers often come from a technical background within development, usually with knowledge of Python and Java. "They are able to get behind the code and take a deep dive in to see what performance issues might occur from vulnerabilities and what tweaks they can make," Zafarino said. They also make sure employees are up to date on security best practices.

3. CISOs

The chief information security officer (CISO) helms a company's cybersecurity strategies. "With all of these changes happening, it's important for companies to make sure they have the right leadership in place and bring in people who are experts in the field," Zafarino said.

In the past, a networking engineer or programmer might have handled cybersecurity on the side. Today, companies want an experienced CISO or security director to lead their efforts. "They are able to come in and

give the right strategy because they have gone through the gauntlet and seen what happens," Zafarino said. "They have worked their way up to the top and know the needs and how to address issues and the best tech to use. They are true subject matter experts. Clients are making sure they have these people in place so they are getting the right strategy and staying ahead of the curve."

Companies are also looking for leaders who aren't afraid to point out issues and offer solutions to fix them. They also need to be future-minded and always looking into how they will continuously grow their approach to security and add new functions, be they tools or employees.

Looking to the future

Zafarino predicted that we will see these same positions in demand going forward into 2018. "We may see a heavier focus on engineering and analysts, and a lot of companies are probably going to be looking for designated leadership with cybersecurity," he said. "They'll also be making sure the right infrastructure is in place, as companies are starting to realize that everyone is a potential threat, and taking measures as a result."

However, with so few available cybersecurity engineers, many companies are taking inexperienced people and training them, Zafarino said.

"For lower-level professionals, companies need to consider if they want to pay a premium for an analyst to get every skillset they're looking for or if they want to invest in trainings and seminars," Zafarino said. If you chose the latter, it's key to bring in a consultant for a short amount of time to help get the employee up to speed. "In the long term, that person is probably perfect, especially if you don't have the money at hand," he said. "If you do, you absolutely want to go with the more senior resource, and you can bring in lower-level people along the way."

Zafarino said he commonly sees two paths to becoming a cybersecurity professional. In the first, a person comes from a computer science background and can usually command a higher salary. In the second, a person comes from a networking or helpdesk background and works their way up to systems administrator by taking basic security courses. They tend to hold lower-level security analyst positions, as opposed to security engineers, who usually have a computer science background.

If you need to fill a hole immediately, Zafarino recommended hiring a consultant, who may be more readily available and cost effective.

"Since the threats keep coming more frequently, if you're looking to hire somebody, you probably want to do it sooner rather than later," Zafarino said.

Learn cybersecurity basics with these YouTube videos

By Dan Patterson

Last year, global cyberwar went mainstream. Banks were robbed by digital criminals, Yahoo confessed to losing half a billion consumer records, foreign attacks leaked documents from the Democratic National Committee and presidential candidate Hillary Clinton, and thousands of small businesses and enterprise companies lost millions of dollars.

Yet cybersecurity is complex, and learning the fundamentals—how hacking works, what attackers want, and how to protect against a data breach—is a daunting prospect for everyone from curious amateurs to IT pros. Even organizations as security-minded as banks "only cover about half of what really matters," said Ernst & Young cybersecurity expert Ertem Osmanoglu in an interview. "Cyber is truly a business issue that needs to be a bigger part of the end-to- end business workflow."

Osmanoglu acknowledges that technology evolves quickly and that 100 percent security is impossible. "Therefore, organizations must be capable of immediately dealing with incidents to minimize loss," he said, and advised organizations of all sizes to leverage new technologies to improve organizational understanding of cyber risk. "While new technologies will allow organizations to detect and respond to threats in real time, organizations should prioritize protection of high value assets. Information protection can seem overwhelming to executives, but allocating additional dollars towards crown jewels is a place to start."

From lessons on how encryption works to the tactics hackers use to attack systems, the edifying and essential videos listed below will help you and your organization better understand the fundamentals of cybersecurity.

- Cybersecurity 101
- Cybersecurity for small business
- Enterprise cybersecurity
- How end-to-end encryption works
- Cyberdefense
- Training cyber-warriors
- Social engineering

Five essential cybersecurity podcasts for IT professionals

By Dan Patterson

From the rise of ransomware to the blooming IoT exploit market, in the coming months security professionals at organizations as diverse as government agencies, enterprise companies, and SMBs will face a growing number of cybersecurity threats.

Because podcasts are both timely and convenient, they're a great way for IT pros to navigate the ever-shifting sands of cybersecurity trends and stay connected to communities of likeminded experts and enthusiasts.

This is a list of essential security podcasts curated to cover a diverse range of topics. Shows like Security Now and Risky Business analyze security news and headlines. Defensive Security and Exploring Information Security are beefy conversations about enterprise and business security trends. And the Social Engineer Podcast is a roundtable discussion about penetration and pretexting tactics.

Although these are some of the most informative and interesting cybersecurity podcasts, this is far from a comprehensive collection of shows. Still, it's definitely a good place to start.

1. Security Now

Security Now is one of the longest-running, most-respected security podcasts. Host Steve Gibson coined the phrase "spyware" and is revered in the security community for writing early anti-malware software. Security Now is a program for both news and tech junkies and provides analysis and detailed technical dissection of security headlines.

- URL
- iTunes

2. Risky Business

Produced by radio host Patrick Gray, Risky Business is an award-winning news program targeted at IT professionals. The program provides context for top security headlines and routinely features guest-host experts who share nuanced details about the state of global hacking, defensive tactics for businesses, and emerging cybersecurity trends.

- URL
- iTunes

3. Defensive Security

Not your typical vanilla tech podcast, Defensive Security is a nerdy but head-banging romp through hot malware trends that threaten SMBs and enterprise companies. Hosts Jerry Bell and Andrew Kalat are well-

versed in technical components of network security and work hard to articulate tangible lessons from data breaches for business listeners.

- URL
- iTunes

4. Exploring Information Security

Exploring Information Security is, as the program's name states, an exploration of the IT security space. Host Timothy De Block brings listeners into security culture by conducting interviews with thought leaders, live reports from conferences like DerbyCon, and technical explainer conversations about topics like cryptography, DDoS attacks, and threat modeling.

- URL
- iTunes

5. The Social-Engineer Podcast

Humans are often the weakest link in an organizational security chain. Social engineering, a time-tested hacker tactic, is the practice of tricking someone into revealing sensitive information like network passwords. The Social-Engineer Podcast is an amalgamation of indie music, deep interviews with security experts, and a topical roundtable discussion about pretexting strategies companies are most likely to encounter.

- URL
- iTunes

Five audiobooks for cybersecurity pros

By Dan Patterson

“Sometimes I hack from coffee shops. I use a few custom scripts to sniff packets flowing over the open Wi-Fi connections. You can learn a lot about someone from watching what they share, who they talk with, and the files they save,” said S1ege, the leader of Ghost Squad Hackers. “I hack for good causes, but other hackers profit from selling personal information and exploits.”

Life is digital, and it’s easily hacked. Cybersecurity is no longer a niche tech topic. Consumers, government agencies, small businesses, and enterprise companies possess sensitive data and are all vulnerable to hacks and cyberattacks. “What I do is technical, but it doesn’t have to be,” S1ege explained. Common tactics like phishing and pretexting prey on sloppy email and protocol habits and manipulate human users to divulge passwords and other sensitive data. “Hackers exploit ignorance as much as they do technical loopholes,” S1ege said.

To protect against a hacking disaster S1ege insists that knowledge is power, and that the best approach is holistic. Although cybersecurity solutions that work for one company may not work for everyone, protecting yourself is made easier by learning how systems function, the types of entities perpetrating attacks, and what hackers want.

“I taught myself to code, but that’s because I read a lot,” the hacker said. Pick up a book, he recommends, and if you don’t have time to sit and read, audiobooks can transform your commute, travel time, or workout into a productive edification session.

This list of cybersecurity audiobooks, though far from comprehensive, provides an informative and accessible introduction to the history of hacking, who hacks and why, how encryption works, and the future of cyberdefense.

Hackers: Heroes of the Computer Revolution by Steven Levy

The term “hacker” originated at MIT and was used to describe particularly adept FORTRAN programmers. Later, the term was applied to a bevy of technical problem solvers. Levy’s seminal work chronicles the history of computing—and early hackers— from the 1950s to the 1980s and is an essential read for those curious about the deep roots of modern hackers.

Cryptonomicon by Neal Stephenson

Though a work of fiction, Stephenson’s enormous (and accurate) tome wraps detailed explanations of how encryption works around a compelling story about hackers during World War II, the Cold War, and during the 1990s Dot Com bubble.

The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age by Adam Segal

The stereotype of a hooded hacker hunched over a keyboard is a popular conception but is a misleading one. Hacking is a global enterprise. Companies, countries, and individuals are routinely targeted by nation states and shady corporations in Russia and China. Segal's book is essential to help understand the scope and scale of global cyberwar.

Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon by Kim Zetter

Your secrets are for sale on the Dark Web, and they're worth a lot of money. Zero Day exploits are vulnerabilities known to hackers but unknown to software vendors. A bug in Facebook or Bank of America, for example, could expose sensitive personal information. Zetter's book details the hidden economies that incentivize and fund the malicious hacking industry.

Spam Nation: The Inside Story of Organized Cybercrime—from Global Epidemic to Your Front Door by Brian Krebs

Check your email junk folder and you're likely to find hundreds of messages competing for your attention. Though most of us ignore spam, one errant click could expose your bank account to nefarious cybercriminals. In Spam Nation, Krebs, a well-respected security consultant, explores the history of the spam industry and exposes the companies and criminals responsible for flooding your inbox.

No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State by Glenn Greenwald

After Edward Snowden leaked NSA secrets to journalists, he became the most notorious hacker in the world. Greenwald's book details the tech timeline of Snowden's hack, how the former Booz Allen contractor duped his colleagues to reveal sensitive data, and how encryption kept the hacker and the journalists secure while reporting the story.

New training platform uses real-world situations to train cybersecurity experts faster

By Alison DeNisco

Many enterprises report increasing difficulties finding skilled cybersecurity professionals, research shows. Some 55% of US organizations report that open cyber positions take at least three months to fill, while 32% said they take six months or more, according to a recent report from the nonprofit ISACA. And 27% of companies said they are unable to fill cybersecurity positions at all.

The shortage—expected to reach 1.8 million jobs by 2022—has led some organizations to turn to training internal candidates to take on these roles.

> "The person is doing a real thing—attacks are happening in real-time, and the person has to respond."
> —Frank Schettini

"There aren't enough people in the industry to fill jobs, and CISOs acknowledge that they are hiring people who they know don't have the right skills—they are taking whatever they can get," Frank Schettini, chief innovation officer at ISACA, told TechRepublic. The largest issue for CISOs is guaranteeing that they can detect an attack and that they have the right policies in place to mitigate it.

Enter ISACA's Cybersecurity Nexus (CSX) Training Platform, released in April. The program is the first of its kind, the nonprofit claims, and offers 100 hours of on-demand, real-world training to build technical skills that help staff combat real threats.

Most cyber training programs remain knowledge-based, Schettini said: An employee sits in a classroom or reads a book. But the CSX training labs place participants in real situations and are configured with real firewalls, web servers, database servers, and other tools.

"The person is doing a real thing—attacks are happening in real-time, and the person has to respond," Schettini said. The program also offers an assessment tool: With each step the participant takes to mitigate a threat, they are given a score on how well they completed the task. Therefore, CISOs or hiring managers can see not only that the person passed or failed, but what areas they succeeded in and where they might need additional training.

The program offers beginner, intermediate, and advanced training situations, ranging from managing networking to ransomware. It is also browser-based, so it can run on enterprise computers without downloading any software.

"There is a huge difference between thinking you know and demonstrating it," Schettini said. "We see it as a tool for organizations struggling to retain their cybersecurity professionals as well—here's a platform they can leverage so they are constantly updating their skills, and an investment the organization makes in them."

The program may come at an opportune time, as enterprises are investing more heavily in cybersecurity training now than in the past, according to a recent report from testing provider Pearson VUE. Among 6,605 US IT professionals surveyed in the last year, there was a 48% increase in those taking security training and a 60% increase in those taking security exams, compared to the year before.

Rise of the "accidental" cybersecurity professional

By Alison DeNisco

With an extreme shortage of trained cybersecurity professionals, it's becoming increasingly common for people—especially women—to enter the field from other careers, including IT, law, compliance, and government. These employees form a group of "accidental" cyber professionals who are filling the need for cyber professionals and offering a different view on security threats.

Job postings in the cybersecurity field have gone up 74% over the past five years—a Cisco report estimates that there are currently 1 million unfilled cybersecurity jobs worldwide. US News and World Report ranked a career in information security analysis fifth on its list of best technology jobs. Average salaries nationally are $88,890 and significantly higher in cities such as San Francisco and New York.

"The job prospects are excellent," said Deborah Hurley, a professor for Brown University's executive master in cybersecurity program. "The demand far outstrips the supply."

Yet women make up only 11% of the world's information security workforce, according to the Women's Society of Cyberjutsu, and just 1% of its leadership.

Part of the reason for this is that there are fewer women in technology in general, Hurley said. "Sometimes it's perceived that the only way of entering cybersecurity is through the technical door, but that's not the case," she said. Hurley started her career as a lawyer and launched the Working Group on Innovation and Technology Policy at the Organization for Economic Cooperation and Development (OECD).

Cybersecurity involves knowledge in tech, human behavior, finance, risk, law, and regulation. "Whatever a person's talent, with people, administration, management, education, or technology, there is almost certainly an aspect of cybersecurity for which their skills and experience are needed," Hurley said.

An interdisciplinary field

Cybersecurity is inherently interdisciplinary. "One thing I've done over and over is bring people from different disciplines into a room, to create a common vocabulary and work through a particular issue or problem that needs to be resolved," Hurley said.

And depending on your background, you may be able to make the leap to security within your own company. "There are tons of opportunities in cyber and many doors of entry. Whatever doorway you come through, you will be working with colleagues from many disciplines and becoming more expert."

Shelley Westman, senior vice president of alliances and field operations at Protegrity, started her career as a lawyer. She left the field and went to work at IBM in a number of roles ranging from procurement to product

management. Eventually, she was assigned a role in hardware security. “I knew nothing about security and had to self-teach everything,” she said. “I fell in love with the space—it’s very analytical and very fast moving.”

At IBM, she started the group Women in Security Excelling (WISE), which grew to 850 members.

“It’s a myth in the industry that you have to be technical to be in the field of cyber,” Westman said. “We need people who have deep analytical skills, who can talk to clients and translate technical speak to business value.” That includes marketing and finance pros as well. “It’s an end-to-end business.”

It also requires strong communication skills and the ability to work as a team. “This is not a business where you can get things done by yourself,” Westman said.

Since cyber is a relatively new field, it makes sense that women in the mid to late stages of their careers started in another area and made the move, said Sherri Ramsay, senior advisor at CyberPoint International and member of the board of directors for the National Women in Cybersecurity Conference. “What you want to see is many more younger women choosing to go into that field.”

The STEM issue

The dearth of women in cybersecurity and technology in general starts as early as middle school, when many young women opt out of STEM courses, said Deidre Diamond, founder and CEO of CyberSN and #brainbabe.

“We’re behind in marketing and representing all of the jobs that exist—our schools have no idea about all of these jobs,” Diamond said. “It’s starting to change, because there is so much money to be made in this business. When it’s sold correctly, women will flock to it.”

Westman said she has had a similar experience. “When I talk to a lot of young girls, they’ve never heard of cybersecurity as a career path—they have a picture in their mind that cybersecurity involves sitting in a dark room by yourself working alone chasing down hackers and bad guys. They don’t seem to be interested in that, but it’s a misperception.”

While undergraduate cybersecurity programs are growing, it’s difficult for them to draw in enough students to meet demand and to keep up to date on all the latest threats, Ramsay said.

“It’s going to take government, industry, and academia to partner together in ways they’ve never done before,” she said, to ensure that people go into the field and are trained appropriately.

Making sure that women enter the field also helps businesses succeed. “It’s proven that the way men and women think about and solve problems is different,” she said. “Because cyber challenges are so difficult and complex, we need to bring all these different ways of thinking about problems to the table.”

How to make the switch

Lisa Kendall, marketing and media manager of CyberSN and #brainbabe, parlayed prior marketing experience and additional cyber training into her current role. “Take what you already know how to do and see what’s out there for you,” she said. “Cybersecurity companies are made up of dozens of different roles and only a handful are technical. Security orgs need sales, marketing, HR, operations, account management, and many other professionals, and all the security industry knowledge needed can be learned on the job.”

Women are much more likely to self-exclude when job searching, Kendall said. “Instead of assuming you can’t do the job, take a chance and put yourself out there. If you can paint the story for the hiring team using your cover letter and a thoughtful resume, you can often get in the door for an interview.”

Different companies have different requirements for entry, Westman said. She recommends reading about the field and finding coding or cybersecurity courses online. (Find certifications and degree programs here.) You can also reach out to your company’s current cybersecurity professional and ask to shadow them.

Companies should look at their current cybersecurity assets for gaps and look for people in the company to fill them, Hurley said. For example, someone from human resources could potentially spearhead employee cybersecurity training.

Westman said that women and men in the industry must be allies in advocating for the profession and get involved in mentoring and speaking to groups of young people to raise awareness of the field. “Be public about why you love the field of cybersecurity. If girls don’t see people like them in the field, they are not going to be interested in going into it.”

About TechRepublic

TechRepublic is a digital publication and online community that empowers the people of business and technology. It provides analysis, tips, best practices, and case studies aimed at helping leaders make better decisions about technology.

Resources

Subscribe to our free newsletters: Stay on top of business technology trends, learn about innovative new products, and hone your skills with our how-to's and tutorials.

Check out the TechRepublic discussion forums: Touch base with your peers and share tips, advice, solutions, and opinions.

Catch the latest videos and photo galleries: Our video library offers interviews with entrepreneurs, IT pros, and CXOs; short clips on the latest tech news; and overviews of emerging technologies. Our galleries offer a look at everything from the hottest mobile devices to autonomous cars to the gadgets, tools, and accessories that are headed your way.