LAUNCHING A CAREER IN CYBERSECURITY: AN INSIDER'S GUIDE

By Alison DeNisco Rayome

TechRepublic

INTRODUCTION

As cybercriminals grow more sophisticated and news of major breaches reach headlines nearly daily, cybersecurity professionals are in high demand: There are currently 1 million unfilled cybersecurity jobs worldwide, Cisco found. By 2022, that number is expected to rise to 1.8 million open jobs, as predicted by the Center for Cyber Safety and Education and ISC(2).

Employees who take on these jobs play a key role in the enterprise, as the average cost of a data breach worldwide is now $3.62 million, according to IBM Security and the Ponemon Institute.

A job in cybersecurity can also command a high paycheck: The average salary for an information security analyst in the US is $92,600, according to the US Bureau of Labor Statistics, and it's significantly higher in cities such as San Francisco and New York.

The shortage of trained cybersecurity professionals has led many organizations to seek nontraditional candidates to fill these roles. To help those interested in the field better understand how to break into a career in cybersecurity, we've pulled together the most important details and resources.

EXECUTIVE SUMMARY

- **Why is there an increased demand for cybersecurity professionals?** Cybercrime has exploded in the past couple of years, with major ransomware attacks such as WannaCry and Petya putting enterprises' data at risk. To protect their information and that of their clients, companies across all industries are seeking cyber professionals to secure their networks.
- **What are some of the cybersecurity job roles?** A career in cybersecurity can take the form of various roles, including penetration tester, chief information security officer (CISO), security engineer, incident responder, security software developer, security auditor, and security consultant.
- **What skills are required to work in cybersecurity?** The skills required to work in cybersecurity vary depending on the position and company, but generally may include penetration testing, risk analysis, and security assessment. Certifications, including Certified in Risk and Information Systems Control (CRISC), Certified Information Security Manager (CISM), and Certified Information Systems Security Professional (CISSP), are also in demand and can net you a higher salary in the field.
- **Where are the hottest markets for cybersecurity jobs?** Top companies including Apple, Lockheed Martin, General Motors, Capital One, and Cisco are all hiring cybersecurity professionals. Industries such as healthcare, education, and government are most likely to suffer a cyberattack, which will probably lead to an increase in the number of IT security jobs in these sectors.

- **What is the average salary of a cybersecurity professional?** The average salary for a cybersecurity professional depends on the position. For example, information security analysts earn a median salary of $92,600 per year, according to the US Bureau of Labor Statistics. Meanwhile, CISOs earn a median salary of $212,462, according to Salary.com. Salaries are significantly higher in certain cities, such as San Francisco and New York.
- **What are typical interview questions for a career in cybersecurity?** Questions can vary depending on the position and what the specific company is looking for, according to Forrester analyst Jeff Pollard. For entry level and early career roles, more technical questions should be expected. As you move up the ranks, the questions may become more about leadership, running a program, conflict resolution, and budgeting.
- **Where can I find resources for a career in cybersecurity?** ISACA, ISC(2), ISSA, and The SANS Institute are national and international organizations where you can seek out information about the profession as well as certification and training options. A number of universities and online courses also offer cybersecurity-related degrees, certifications, and prep programs.

Additional resources

- Report: The top 5 cybersecurity threats of 2017 (TechRepublic)
- Special report: Cybersecurity in an IoT and mobile world (free PDF) (TechRepublic)
- Essential reading for IT leaders: 10 books on cybersecurity (free PDF) (TechRepublic)
- Defending against cyberwar: How the cybersecurity elite are working to prevent a digital apocalypse (free PDF) (TechRepublic)
- Cybercrime and cyberwar: A spotter's guide to the groups that are out to get you (ZDNet)

WHY IS THERE AN INCREASED DEMAND FOR CYBERSECURITY PROFESSIONALS?

Cybercrime has exploded in the past couple of years, with major ransomware attacks such as WannaCry and Petya putting enterprises' data at risk. The rise of the Internet of Things (IoT) has also opened up new threat vectors. To protect their information and that of their clients, companies across all industries are seeking cyber professionals to secure their networks.

However, many enterprises face difficulties filling these positions: 55% of US organizations reported that open cybersecurity positions take at least three months to fill, while 32% said they take six months or more, according to an ISACA report. And 27% of companies said they are unable to fill cybersecurity positions at all.

Cybersecurity remains a relatively new field compared to other computer sciences, so a lack of awareness is part of the reason for the talent shortage, according to Lauren Heyndrickx, who is now CISO at JCPenney. Misconceptions about what a cybersecurity job actually entails are common and might be part of the reason few women and minorities go into the field, she said. Still, enrollment in computer science programs has increased tremendously in the past couple years, and many schools are adding cybersecurity majors and concentrations, said Rachel Greenstadt, associate professor of computer science at Drexel University.

Additional resources

- 5 reasons your company can't hire a cybersecurity professional, and what you can do to fix it (TechRepublic)
- Cybersecurity spotlight: The critical labor shortage (Tech Pro Research)
- Report: 57% of businesses can't find enough IT security pros (TechRepublic)
- Report: Despite growing security threats, CXOs struggle to find cybersecurity professionals (TechRepublic)
- Cybersecurity: Two-thirds of CIOs say threats increasing, cite growth of ransomware (TechRepublic)
- These women want to fix cybersecurity's massive gender gap (CNET)
- International Women's Day: A plea to the infosec community (ZDNet)
- Gender gap: Why information security needs more women (TechRepublic)
- 16 tech jobs with the largest gender gaps (TechRepublic)

WHAT ARE SOME OF THE CYBERSECURITY JOB ROLES?

Cybersecurity jobs span a number of roles with a variety of job functions, depending on their title as well as an individual company's needs.

In-demand roles include penetration testers, who go into a system or network, find vulnerabilities, and either report them to the organization or patch them themselves. Cybersecurity engineers, who often come from a technical background within development, dive into code to determine flaws and how to strengthen an organization's security posture. Security software developers integrate security into applications during the design and development process.

Computer forensics experts conduct security incident investigations, accessing and analyzing evidence from computers, networks, and data storage devices. Security consultants act as advisors, designing and implementing the strongest possible security solutions based on the needs and threats facing an individual company.

At the top of the chain, CISOs helm a company's cybersecurity strategy and must continuously adapt to battle the latest threats.

Additional resources

- Rise of the CISO: Why the C suite needs a security chief (TechRepublic)
- Job description: Identity access management specialist (Tech Pro Research)
- Job description: Computer forensic analyst (Tech Pro Research)
- Job description: Information security analyst (Tech Pro Research)
- Job description: Security architect (Tech Pro Research)

WHAT SKILLS ARE REQUIRED TO WORK IN CYBERSECURITY?

The skills required to work in cybersecurity vary depending on what position you enter and what company you work for. Generally, cybersecurity workers are responsible for tasks such as penetration testing (the practice of testing a computer system, network, or web application to find vulnerabilities that an attacker could exploit), risk analysis (the process of defining and analyzing the cyber threats to a business and aligning tech-related objectives to business objectives), and security assessment (a process that identifies the current security posture of an information system or organization and offers recommendations for improvement).

Certifications in cybersecurity teach these and other valuable job skills and often lead to higher salaries in the field. Those who hold certs like Certified in Risk and Information Systems Control (CRISC), Certified Information Security Manager (CISM), and Certified Information Systems Security Professional (CISSP) are currently in high demand.

Cybersecurity jobs don't necessarily require developer skills or a degree, Pollard said. "You don't need a bachelor's degree in a specific field to be great at security; in fact, you don't necessarily need [a degree] at all," he said. "Recognize that cybersecurity is a skill, and teach people the profession of enterprise security. That means treating it like an apprenticeship or training program."

Cybersecurity is an interdisciplinary field that requires knowledge in tech, human behavior, finance, risk, law, and regulation. Many people in the cybersecurity workforce enter the field from other careers that tap these skills and translate them to cyber.

"If you have security skills, there are plenty of opportunities available for you," Pollard said. "If you have an interest in security and perhaps have a nontraditional background but are willing to learn, opportunities are certainly open from that perspective as well."

Additional resources

- Rise of the "accidental" cybersecurity professional (TechRepublic)
- Cybersecurity specialisation status up for grabs with new ACS accreditation program (ZDNet)
- Ethical hackers: How hiring white hats can help defend your organisation against the bad guys (TechRepublic)
- The next generation of cybersecurity professionals is being created by the Girl Scouts (TechRepublic)
- 10 bad habits cybersecurity professionals must break (TechRepublic)
- Information Security Certification Training Bundle (TechRepublic Academy)
- Learn Website Hacking and Penetration Testing From Scratch (TechRepublic Academy)

WHERE ARE THE HOTTEST MARKETS FOR CYBERSECURITY JOBS?

Executives across almost every industry worldwide are looking to bolster their security standings and are hiring professionals to help them do so. Large enterprises including Apple, Lockheed Martin, General Motors, Capital One, Cisco, Intel, and Boeing all had at least 20 job postings for cybersecurity roles from October 2016 to December 2016, according to a report from Indeed.

Industries such as healthcare, education, and government are most likely to experience a cyberattack, and cybersecurity jobs are likely to increase across those fields as well.

Demand for cybersecurity professionals will only continue to increase in the coming years, experts say. By 2022, there will be 1.8 million open jobs in this field, according to the Center for Cyber Safety and Education and ISC(2).

It's going to be especially important for young people to enter the field in the coming years, said Wesley Simpson, COO of ISC(2). Currently, only 7% of cybersecurity workers are under age 29, and 13% are between ages 30 and 34. The average age of cybersecurity professionals is 42.

"Over the next 10 years, we will have a large population of cyber professionals starting to retire," Simpson said. "We don't have a good plan to backfill those large numbers of folks starting to leave the industry. We need to be able to educate and bring awareness to all facets of cybersecurity, and [send a message] that regardless of whether you have a technical degree, it's a great, diverse, lucrative career for folks to get into."

Additional resources

- Help wanted: Universities double down on security to help fill 1 million open jobs (TechRepublic)
- Top 10 companies hiring cybersecurity professionals (TechRepublic)
- The world needs more cybersecurity pros, but millennials aren't interested in the field (TechRepublic)
- The 3 most in-demand cybersecurity jobs of 2017 (TechRepublic)
- Cyber Soldiers: White-hat hackers (CBS News)
- One in three cybersecurity job openings go begging, survey finds (ZDNet)

WHAT IS THE AVERAGE SALARY OF A CYBERSECURITY PROFESSIONAL?

The average salary for a cybersecurity professional depends on the position and the company. For example, information security analysts earn a median wage of $92,600 per year, according to the US Bureau of Labor Statistics. Meanwhile, CISOs earn a median salary of $212,462, according to Salary.com. Salaries are significantly higher in certain cities such as San Francisco and New York.

Demand for skilled cybersecurity professionals has made the field "a seller's market," according to Pollard. Skilled job candidates are more able to negotiate salary, benefits, and perks such as working remotely than in the past, according to Stephen Zafarino, senior director of recruiting at staffing agency Mondo.

Additional resources

- Top 10 hottest IT jobs for 2017 (TechRepublic)
- The 10 best tech jobs that pay the highest salaries (TechRepublic)
- CIOs expect to increase hiring in 2017, here are the tech jobs that top their list (TechRepublic)

WHAT ARE TYPICAL INTERVIEW QUESTIONS FOR A CAREER IN CYBERSECURITY?

Hiring security professionals can often be a difficult task, said Charles Gaughf, security lead at ISC(2). "Depending on your organization's structure you may be looking for a very specific knowledge set or skill, but most likely the need is for a competent professional who is well versed in a variety of technology, who is driven, inquisitive, and honest," he said. "That is why it is a good idea to cater your questions to ascertain these qualities. It is also a good idea to throw out some questions that make the candidate think and that you know haven't been practiced prior to the interview."

Questions can vary depending on the position and what the specific company is looking for, Pollard said. For entry-level and early career roles, more technical questions should be expected. As you move up the ranks, the questions may become more about leadership, running a program, conflict resolution, and budgeting.

An opening question to test the candidate's ability to think on the spot might be, "How do you build a botnet?" requiring them to work out how they would infect, control, and coordinate a botnet from scratch—instantly putting them in the shoes of the attacker, Gaughf said. Then they might be asked, "How would you defend against your botnet?" to gain the other perspective.

In an initial interview, Pollard said, a candidate can also expect technical questions, such as:

- What are some ways malware can evade detection by antivirus products?
- What is a cross-site scripting (XSS) attack and how does it work?
- Outside of XSS, what are a few other examples of web application attacks?
- What is a man-in-the-middle attack and how can it be prevented?
- What is the difference between TCP and UDP? What kind of use cases are better for UDP?

Candidates may also expect questions to determine how they keep up with the industry, Gaughf said, such as:

- Do you belong to any local security groups?
- How do you keep up with cybersecurity news?
- What security podcasts do you listen to?

After an initial interview, candidates often move forward to a simulated exercise of doing the job, which may be simple or complex, depending on the role. Employers are usually looking for candidates who can explain their decision making process, rather than those who complete the task perfectly.

"I might hand them some log data and ask questions about the contents of the data. I might hand them a forensic capture from a system and ask them to perform light investigative work and answer details about the attacker," Pollard said. "If the person was going to be a developer I might ask them to write some code that could parse through data. If the person was going to be a penetration tester, I might hand them a basic web application and ask them to attack it."

After that point, the candidate may have a final interview to explain their solution, reasoning, and methodology.

"For both parties—the company and the candidate—this is lots of work," Pollard said. "And it doesn't fit the traditional interview arrangement where you sort through a mountain of resumes, pick some people to

interview, and then rely on a series of 30-45 minute questions, and move people forward based on some combination of responses, instinct, and emotion."

Additional resources

- 10 questions job seekers can expect in a cybersecurity interview (TechRepublic)
- Five traits employers should look for when hiring cyber security professionals (TechRepublic)
- Landing that infosec job: These experts share their best career advice (ZDNet)
- How to answer tough interview questions: 8 tips (TechRepublic)
- 8 ways to be less nervous about your next job interview (TechRepublic)
- Coding school graduates: Are they worth hiring? (TechRepublic)
- Google for Jobs is ready to get you hired (TechRepublic)

WHERE CAN I FIND RESOURCES FOR A CAREER IN CYBERSECURITY?

Several national and international organizations for cybersecurity professionals and those interested in the field exist. ISACA, ISC(2), ISSA, and The SANS Institute offer information about the profession, as well as research and certification and training program options.

You can reach out to the person in your organization who is currently responsible for cybersecurity and see if you can shadow them or become a mentee.

A number of universities and online courses also offer cybersecurity-related degrees and certifications.

Additional resources

- Five essential cybersecurity audiobooks (TechRepublic)
- Five essential cybersecurity podcasts for IT professionals (TechRepublic)
- Learn cybersecurity basics with these essential YouTube videos (TechRepublic)
- Essential follows: Information security experts on Twitter (TechRepublic)
- New training platform uses real-world situations to train cybersecurity experts faster (TechRepublic)
- Women in cybersecurity: IBM wants to send you to a hacker conference for free (TechRepublic)

CREDITS

Editor In Chief
Bill Detwiler

Editor In Chief, UK
Steve Ranger

Associate Managing Editor
Mary Weilage

Senior Editor
Alison DeNisco Rayome

Editor, Australia
Chris Duckett

Senior Features Editor
Jody Gilbert

Senior Writer
Teena Maddox

Chief Reporter
Nick Heath

Staff Writer
Macy Bayern

Associate Editor
Melanie Wachsman

Multimedia Producer
Derek Poore

Cover image
iStock/ metamorworks

TechRepublic

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.

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.