techopedia

Cybersecurity: The Big, Profitable Field Techies Are Overlooking

By Tara Struyk (/contributors/tara-struyk), December 11, 2013

Takeaway: The cybersecurity field is growing, profitable and full of possibility.

If we had to pinpoint one tech career with truly great prospects over the next couple of years, it'd be cybersecurity (/definition /24747/cybersecurity). Demand for cybersecurity pros is huge. According to the Bureau of Labor Statistics, careers in network systems and information security are expected to grow by 53 percent through 2018. The pay isn't bad either. A survey by Semper Secure (http://www.sempersecure.org/images/pdfs/cyber_security_census_press_release.pdf) in August 2013 found that those who work in cybersecurity security were earning $116,00 per year, on average.

What is lacking in this field is professionals to take these jobs. According to a survey released by Raytheon (http://raytheon.mediaroom.com/index.php?s=43&item=2435) in October 2013, only 24 percent of millenials have any interest in cybersecurity as a career. That can be at least partly attributed to the fact that many people just aren't sure what this career track entails. So, we asked cybersecurity professionals to tell us how they got into the field - and why they think it should rank higher on job seekers' list of potential careers.

We Asked: Why Cybersecurity?

"There's a huge demand for a qualified national cybersecurity workforce, and little supply, which is surprising given the challenging and varied types of work, flexible work options, and the chance to make a difference. ***Lets not forget, there's also tremendous pay and advancement opportunities, even for entry-level technicians.***"

-Casey W. O'Brien, director and principal investigator at the National CyberWatch Center (http://www.cyberwatchcenter.org/)

"Cybersecurity is one of today's most important, interesting and challenging areas to work in. From administrating security solutions or running operations, helping defend a network against an attack or investigating suspicious activity, the cybersecurity field offers a wide range of different job opportunities for different skill sets. If you are the kind of person who is always questioning how things are being done and how to improve them, someone who wants to find out how things work internally and what it takes to make them break, you could move into security research ... ***it is never boring.***"

-Toralv Dirro, security strategist at McAfee
(http://www.mcafee.com/)
"Cybersecurity professionals are important to the foundation of an organization and have ample opportunity to advance and grow while working with the most innovative and fastest evolving technologies. They are responsible for protecting all critical assets, keeping networks secure and protecting intellectual property and data. While challenging, the work is engaging and rewarding. *It involves working beside some of the brightest people working on cutting edge technology*. What other career would give you the opportunity to protect an organization's infrastructure and the people inside it?"

-John Trobough, president of Narus (http://www.narus.com/)

"[Cybersecurity] is an ever-evolving field where you need to remain an up-to-date, life-long learner in order to be relevant and competitive. It's an integral part of operational risk management, with very promising organizational visibility and evolution. ***It's a rather young field where intra- and entrepreneurship are much needed and where complex issues need innovative and bold thinking.***"

-Hadi El-Khoury, founding member of the ISSA (http://www.issa.org/) France Chapter

"Cybersecurity is a great field for those who like a challenge. ***Stopping malware is a game of using your head*** while keeping in mind the amount of money being spent to build up defensive measures."

-Michael Patterson, CEO of Plixer
(http://www.plixer.com/)

"You don't get into cybersecurity for the money or job opportunities. You get into it because you love to do it. You get into it because you live and breathe computers; you think in code. At my university I have seen hundreds of Millennials come into the lab and get excited that they are "hacking" but become quickly discouraged at the complexity. ***The learning curve is so steep, the only thing you can do is keep climbing or jump off.***"

-Mark Kikta, security consultant at VioPoint (http://www.viopoint.com/)

Getting Into and Working In Cybersecurity

"What does it take [to work in cybersecurity]? Curiosity. A burning desire to understand how things work. ***A mischievous streak.*** Creativity. The ability to teach yourself new things without a lot of guidance. Dogged persistence. Communication skills."

-Chris Eng, vice president of research at Veracode (http://www.veracode.com/)

"Are you truly competitive? Do you enjoy the lessons of defeat as much as the thrill of winning? ***Do people refuse to watch films with you, because you figure out the twist ending 10 minutes into the film?*** We could use you in information security. Every day we wake up to a job where the rules have changed, and something new waits to be discovered by the curious."

-Conrad Constantine, senior research engineer at AlienVault (http://www.alienvault.com/)

"In cybersecurity, you get to wear a the proverbial white hat, since you're trying to prevent cybercriminals from doing their illegal activities. But then again, ***to stop a hacker, you've got to think like a hacker.*** Your hat will have a touch of gray as you work the edges, possibly getting into chat rooms with hackers, etc. "

-Craig Kensek, senior manager at AhnLab (http://www.us.ahnlab.com/)

"Working in cybersecurity requires an aggressively analytical mind behind a thoughtful countenance. It is a field that offers a large list of options where someone can find a niche and break the mold of what it is to be successful, while simultaneously rewarding institutional knowledge and historical perspective, all of which is good for long-term employment. It attracts people who enjoy physics, math, engineering, philosophy, art, creative writing, reading, economics and anything having to do with technology. I***f you have an appreciation for good grammar and can diagram a sentence in your head then you have the mind that fits well in computer science.***"

-Adam Wosotowsky, messaging data architect at McAfee (http://www.mcafee.com)

"Cybersecurity, as a discipline, is becoming increasingly sophisticated, requiring not only an understanding of the technical implementation of security measures, but also extensive data analysis to monitor networks, detect anomalies and attacks, as well as conduct forensic analysis to understand the genesis of attack ... ***There are several emerging areas in the area of cybersecurity too, including international cyber warfare, policy and legal framework in security, and SCADA security, all of these have tremendous growth potential and are high compensation fields.***"

-Sanjay Goel, director of research for the NYS Center for Information Forensics and Assurance at University at Albany State University of New York (http://www.albany.edu/cifa/)

"***Cyber criminals are getting smarter and more creative by the minute.*** The cybersecurity market is always changing and the demand for talent is relentless. Before getting into this field, it's important for job seekers to understand the role next-generation technologies play in the effort to stay ahead of advanced cyber threats and the blurring lines between physical and digital assets."

-John Trobough, president of Narus (http://www.narus.com/)

"***Cybersecurity jobs can range from a firewall administrator, incident response analyst, auditor, compliance analyst, security consultant, forensic analyst or penetration tester. Each of these jobs comes with a completely different lifestyle.*** Qualifications for a job in a testing or research capacity are hard to nail down. We've found that a passion for security and an obsession with 'deconstructing' things to find how they work (and how they can be abused) is the top qualifier."

-Mike Weber, managing director of Coalfire Labs (http://www.coalfire.com/Home)

"To survive or even thrive as an expert in this field often requires a healthy background on how various applications communicate within IP. Malware developers often piggyback reconnaissance messages on port 80 and even 443 these days. For this reason,

knowing what traffic is normal and what traffic is suspicious takes experience when monitoring HTTP and SSL connections."

-Michael Patterson, CEO of Plixer (http://www.plixer.com/)

"***When I interview cybersecurity candidates, the most important thing I'm looking for is the security mindset.*** The ability for a candidate to think divergently, and look at a system not in terms of what it can do, but in terms of how it can be exploited to do that which it was not intended to do, is the key attribute of a candidate that will excel in the field."

-David Campbell, CEO of Electric Alchemy (http://electricalchemy.net/)

"Breaking into security requires a lot of internal motivation. ***It's not the kind of career where you can go to college, get a degree, and find a job.*** A lot of successful people in the industry don't even have four-year degrees. It's about passion; you have to want to spend your own time learning new toolsets and crawling through security blogs. Security is a steep learning curve that never really straightens out, and not everyone can deal with it."

-Ken Smith, staff security consultant for the Profiling & Penetration team at SecureState (http://www.securestate.com/Pages/default.aspx)

"The field of cybersecurity represents a shining light of opportunity both now and in the foreseeable future. It has never been more important or more valued in private industry, and this is an increasing trend. Qualified candidates are in demand, and as a result command compensation commensurate with their experience and capabilities. In short, ***cybersecurity is a field ripe with opportunity, career potential, and reward***."

-Joe Fisher, president at Affinity IT Security (http://www.affinity-it-security.com/)