

## CAREER SPOTLIGHT: What It Takes to Work in Information Security



**Think like a hacker!**

### Have you ever thought about a career in Information Security?

Competition for technical talent is on the rise, and as security becomes increasingly important for nearly every company, positions related to cybersecurity are in high demand.

**According to the Bureau of Labor Statistics, the rate of growth for jobs in information security is projected to increase 37 percent between 2012 and 2022, much higher than the average 11 percent for most occupations.**<sup>1</sup> Although cybersecurity

programs in colleges and universities are growing, security programs offered at schools are currently not as widespread as they

should be for the high level of demand for these positions. The 2015 Stack Overflow Developer Survey estimates 42 percent of developers are self-taught and 55 percent of developers have less than 6 years' experience.<sup>2</sup> The average age for a developer is 20-24 years old, leading to believe there is a large amount of inexperienced developers out there who likely don't know much about secure coding or how to discover vulnerabilities within code. If you're looking to break into this emerging field of cybersecurity, there are a few things you'll need to know.

## What Makes a Good Security Engineer/Analyst?

**To put it simply, a Security Analyst will find the vulnerabilities while a Security Engineer is responsible for fixing them.** Companies take security seriously, so it can be expected that they

take the hiring process seriously as well. Many hiring employers look for the technical skills, but also look at personality to fit the position. **People who are razorsharp, passionate, and have a track record of getting things done fit into a Security Engineer or Analyst position very well.** They need complete knowledge of the system being tested, an imagination to think outside the box, and the "evil streak," which can be described as the drive to think like a hacker and take things to the next level to find the vulnerability and fix them before a hacker takes advantage.

It's imperative you read the latest books on writing secure code and building secure software, and also stay up-to-date with trends in the cybersecurity industry by following popular blogs and influential people on social media. **Security Engineers and Analysts are known for their complex problemsolving skills to combat cyberattacks and prevent hackers from stealing critical information or wreaking havoc on company networks.**

Common skills required for a cybersecurity job role are:

- |   |   |
|---|---|
| <input type="checkbox"/> Advanced malware protection    | <input type="checkbox"/> Application security development |
| <input type="checkbox"/> Incident handling and response | <input type="checkbox"/> Intrusion detection              |
| <input type="checkbox"/> Auditing and compliance        | <input type="checkbox"/> Analytics and intelligence       |
| <input type="checkbox"/> Firewall/IDS/IPS skills        | <input type="checkbox"/> SIEM management                  |
| <input type="checkbox"/> Access/Identity management     | <input type="checkbox"/> Cloud computing/virtualization   |

Not surprisingly, commonly targeted industries including Banking/Finance/Insurance, Information Technology, Government, and Consulting or Professional Services often hire cybersecurity professionals, so a background in one of these industries definitely helps.

## Getting Started as a Security Engineer or Analyst

**If going back to school isn't an option, there's still hope.** While common technical skills are still a must, hands on experience can also help. **A passionate Security Engineer or Analyst will have active Github projects, go to security conferences, and be engaged by commenting on websites like StackOverflow.** Experience and side projects demonstrate how in-depth your working knowledge of cybersecurity really is. There are also a number of certifications available including CISSP, CEH, and others, which some employers will require but others may focus more on experience.

## Is This the Career for Me?

This job position isn't for everyone. A data breach could make or break a business, and it could be your inability to find a vulnerability or your insecure code that causes it. **In the event of an actual data breach or serious attack, you will likely need to deal with high stress levels and be willing to work long hours to remediate the issue.** Although, if you've done your homework, you'll hopefully never experience a serious attack and you can enjoy the new challenges every new day brings when working in Information Security.

1. <http://www.bls.gov/ooh/computerandinformationtechnology/informationsecurityanalysts.htm>
2. <http://stackoverflow.com/research/developerssurvey2015>