August 2019
Volume 14, Issue 8

Careers in Cybersecurity: Learn More or Get Involved!

From the desk of Thomas F. Duffy, MS-ISAC Chair

Technology is expanding its reach over our daily lives and is becoming increasingly necessary in modern society. While change can be daunting, it brings new opportunities that did not exist when we were much younger, or even just a few years ago. This opens the door for new and exciting (not to mention realistic) careers we can chase, like cybersecurity.

Twenty years ago, society and the media focused on the Y2K bug and ensuring computers would survive the transition from 12/31/1999 to 1/1/2000. Currently, technology headlines are dominated by breaches and ransomware attacks, directly impacting people everywhere. It is evident that the cybersecurity field needs capable professionals now more than ever.

You may be interested in becoming one of those people, or know a student or colleague that may have interest in this discipline. Let's explore transitioning into the cybersecurity field, what skills are needed, and what career pathways are available.

Consider the skills and talents you use every day. Aside from technical abilities, many skills that transfer into the field of cybersecurity may surprise you. Communication and writing skills lend to effectively conveying the risk to all levels of an organization. The ability to analyze data gives an advantage when defining metrics. Attention to detail helps when analyzing legislation or conducting digital forensics. See below for more examples of skills:

Soft Skills for Management Positions	Soft Skills for Non-Management Positions	
• Strong leadership skills • Strategic thinker • Long-term planning • Good oral and written communications • Creative problem solving • Capable of handling stress • Ability to multitask • Ability to delegate	• Ability to think outside the box • Ability to work in a team • Analytical thinking • Attention to detail • Capable of handling stress • Creativity • Curiosity • Flexibility	• Interest in cybersecurity/hacking • Communications • Problem solving

As the field of cybersecurity continues to explode, more and more positions and pathways are created. It is important to note that cybersecurity can be broken into two distinct focus areas: security management and security operations. Management focuses on policies, procedures, education initiatives, and the governance around all elements of a security program. Operations on the other hand, focuses more on the technical side of security such as device management, penetration testing, event monitoring, etc. While considering your path, think about which option appeals to you more. The NICE framework is a great career pathing guide as it standardizes career paths and job titles and provides lists of core competencies and skills.

The Cyber Seek careers site provides a place to consider job paths, while also looking at current openings around the United States.

As you explore the above resources and career paths, take a look into the resources below on professional development and training as well:

Federal Virtual Training Environment (FedVTE) – 800+ hours of no-cost cyber training for employees of State, Local, Tribal, and Territorial governments and US veterans.
SANS Institute – Offers paid professional development and certification courses and more
NSA Centers of Academic Excellence – Identified and certified institutions of education recommended for study in cybersecurity

Although cybersecurity was not as common or distinct of a career path in the distant past, we are seeing it more prominently represented as an option in education. The need to introduce children to cybersecurity at a young age becomes critical to help fill the skills gap in the field. See these examples below that can be shared with any young future cyber professionals you may know!

CyberPatriot – For middle school students to learn cybersecurity in team events
Girl Scouts and HPE Cybersecurity Game – For Girl Scouts aged 9-11 to learn cybersecurity
SANS CyberStart – For High School students to learn cybersecurity through challenges/games

These initiatives are gaining interest and are ensuring that kids can envision becoming a cybersecurity forensic investigator, a white hat hacker, or one of the most in demand security consultants in the country.