Cybersecurity & the Job Market

Salim Hariri, Co-Director
NSF Center for Cloud and Autonomic Computing
The University of Arizona
nsfcac.arizona.edu
email: hariri@ece.arizona.edu
(520) 977-7954

Cybersecurity Challenges

- We are rapidly moving toward completely digital world, society, government, and economy
- By 2021, cyber crime and cyber IT damage is projected to cost $6 Trillion annually, compared to $3 Trillion in 2015, according to CSO's State of Cybercrimes 2017 report[1]
- Our current defense tools fail to protect against attacks in spite of drastic increases to fund R&D and deployment of cybersecurity products
  - There are more than 3.8 billion Internet users, up from 2 billion in 2015
  - There are more than 1.2 billion websites, and IoT smart devices are expected to reach 200 billion by 2020 up from 2 billion in 2006

1: CSO. "Top 5 cybersecurity facts, figures, and statistics for 2018." Jan. 2018

Bottom line - Zero unemployment for Cybersecurity Workforce

- There is a significant and growing gap between available corporate and government cybersecurity jobs and the people available to do them.
- Today the US Dept. of Commerce estimates there are around 350,000 cybersecurity jobs currently unfilled. Also, Cybersecurity Ventures estimates 3.5 million cybersecurity jobs will be unfilled globally by 2021
- With cybersecurity jobs in such high demand and skilled professionals in low supply, that makes cybersecurity an excellent career path
- UA Cybersecurity Certificate Program: Network Security, Computer Security, Forensic and Security Analysis, and Cloud and Web Security are designed to help you apply to these unfilled cybersecurity jobs!

1. Cybersecurity Engineer

- The Cybersecurity Engineer was the most in-demand security position for 2018 and 2019 and tops the chart again in 2020. Cybersecurity Engineers are tasked to designing and implementing security systems to stop advanced cyberattacks.
- Cybersecurity Engineer develops security plans and policies, implement solutions, mitigate vulnerabilities, investigate breaches, and respond to security incidents. As the quantity and severity of security threats rise, so does the need for Cybersecurity Engineers to design systems to stop them.
- This position requires a broad base of knowledge and the ability to maintain systems, identify vulnerabilities, track issues, and improve automation. Most Cybersecurity Engineer roles require at least three years of professional experience (depending on the quality and depth of the skillset). A master's degree is expected to become more commonplace, especially for senior-level engineering roles. Certifications are also highly valued in this field, and certifications like the CEH, CISSP, or any security-related GIAC certifications may help win the job.

Average salary: $106,000

Related NICE Work Role IDs: PR-INF001, SP-SYS001

2. Cybersecurity Analyst

- For the second year in a row, the Cybersecurity Analyst role ranks as the first runner-up for most in-demand security position. Cybersecurity Analysts are on the front lines of an organization's cyber defense. With the number of data breaches increasing by over 50% since last year, Cybersecurity Analysts keep constant tabs on threats and monitor their organization's network for any potential security vulnerabilities. Using information collected from threat monitoring tools and other sources, they identify, analyze, and report on events that have occurred or may occur on the network.
- The U.S. Bureau of Labor Statistics expects a 32% growth in hiring for the Cybersecurity Analyst role between 2018 and 2028 – far outpacing the average for the other roles on this list. Since just last year, the total number of job openings for a Cybersecurity Analyst has increased by almost 4,000.

Average salary: $95,000

Related NICE Work Role IDs: PR-CDA-001

3. Network Engineer / Architect

- Making the list for the first time in 2020 is the role of Network Engineer/Architect. Network Engineers/Architects are responsible for implementing, designing, and testing secure, cost-effective computer networks, including local area networks (LANs), wide area networks (WANs), internet connections, intranets, and other data communication systems.
- Network Engineers/Architects are in charge of upgrading software and hardware and planning the implementation of security patches or other defense measures to protect the network against vulnerabilities. Researching new networking technology to better analyze current data and estimate how future organizational growth might affect the network are also important components of this role.

Average salary: $113,500

Related NICE Work Role IDs: SP-ARC-001, OM-NET-001

4. Cybersecurity Consultant

- Holding the same spot for the second year in a row is the Cybersecurity Consultant. The Cybersecurity Consultant plays the role of both an attacker and a defender to exploit vulnerabilities and detect weaknesses in an organization’s computer network, systems, and applications. Typically, this position is not employed by in-house security teams; a Cybersecurity Consultant is usually either a self-employed contractor or works for an external or third-party security consulting firm.
- Cybersecurity Consultant can range from an entry-level to a more intermediate-level cybersecurity position, with most employers looking to see a degree in the field, technical skills, certifications, and potentially work experience conducting similar tasks.
- Since cyber threats are constantly changing, it is not surprising that this position has maintained such a high demand. As the demand for cybersecurity workers has boomed and companies struggle to fill security roles, they increasingly rely on cybersecurity consulting firms to handle their largest, most complex projects. As a result, the need for Cybersecurity Consultants is on the rise among professional services firms.

Average salary: $91,000

Related NICE Work Role ID: N/A

5. Cybersecurity Manager / Administrator

- Cybersecurity Managers/Administrators are typically responsible for implementing and overseeing the cybersecurity program for a given system or network, and many organizations require multiple Security Managers to run specific portions of their enterprise security program.
- Many organizations further break down the cybersecurity manager role into two categories: *program security managers*, which are typically focused on programmatic risk management and mitigation, and *technical security managers*, which oversee specific systems and the teams that manage them (think firewalls, pen testing, encryption, etc.).
- Cybersecurity Manager/Administrator role requires significant work experience and technical expertise, and many employers look for professionals with degrees in cybersecurity or a related field.
- With the rapid growth of enterprise SOCs, organizations will continue to seek out cybersecurity managers to serve as the backbone of their ever-expanding security programs.

Average salary: $105,000

Related NICE Work Role IDs: OV-MGT-001

You don't need to be a hacker to get a high-paying cybersecurity job

- What is necessary or critical in cybersecurity is the ability to analyze, the curiosity, and the desire to understand how things work.
- The University of Arizona Continuing & Professional Education Cybersecurity Program is designed to help obtain these skills

1. **Network Security**
2. **Computer Security**
3. **Penetration Testing**
4. **Cybersecurity Expert**

University of Arizona Continuing & Professional Education Cyber Security Program

Pratik Satam
Research Assistant Professor
The University of Arizona
email: pratiksatam@arizona.edu

Unique Features – Mainly Hands On

- The main differentiating factor of the Continuing & Professional Education Cyber Security Program from other non-credit professional development programs is, we offer students hands on experience, rather than being a theory focused program

- Students will learn to use the tools to monitor actual network traffic, perform cyberattacks like Denial of Service (DoS), DNS based attacks, analyze threats on devices, use tools to secure vulnerable devices

- None of these activities are simulations. The student will perform actual, real attacks on virtual machines that very much behave like real computers or network devices

- These cyber security experiments are provided through our interactive system called: Cybersecurity Lab as a Service (CLaaS) (lab.askcypert.org)

Tools to be learned

- Wireshark, TCPDump, IPTraf, P0F to monitor networks
- OpenVAS for vulnerability analysis
- Linux firewall systems
- Snort Intrusion Detection System to detect attacks on the network
- Nmap to identify the open ports and services on a system
- DnsHijacking an attack to hijack DNS protocol