# 3 Ways Cybersecurity is Uniquely Positioned to Provide a Pathway Into the Tech Industry

Cybersecurity democratizes access to opportunity and creates a global talent win for companies.

May 22, 2021 4 min read

Opinions expressed by *Entrepreneur* contributors are their own.

Breaking into the tech sector remains phenomenally difficult for most of the world. While talent is equally distributed, the pathways to opportunities are most certainly not, evidenced by the lack of cultural, geographic, socioeconomic, gender and racial diversity in the industry.

At a time when the opportunity and income inequality gap continues to widen, cybersecurity is an area of the tech economy that is growing rapidly, pays well and offers an underappreciated pathway into highly skilled and paid work that is relatively accessible for anyone.

This topic is something I know both personally and professionally. My journey into the cybersecurity industry is all the result of practical doing. I am completely self taught, and so is the rest of the global Inspectiv team. The unique structure and pace of the cybersecurity industry means that it is uniquely positioned to provide teams exposure and access to world class talent that they wouldn’t have been able to access before.

# There’s no barrier to entry

One reason cybersecurity is uniquely well suited to democratizing access is that there are no barriers to getting started. Unlike universities or the regulated professions, no one institution or governing body decides who is admitted into the cybersecurity space or decides who gets access to learning the skills needed. With online learning platforms, bootcamps, YouTube videos and the ability to work with people in real time, being highly skilled and self taught is common. Highly skilled global talent that doesn’t have the means to apply and attend a competitive technical program can still be a part of the global tech talent ecosystem.

Regardless of location, education, physical appearance or social network, security researchers can also access real world mentorship and learning opportunities. This usually happens through what is known as “bug bounty” programs. These allow independent security researchers to report bugs to an organization and receive financial rewards, while building their own portfolios and professional networks. No credentials or institutional accreditation is required to get started in a bug bounty program. In fact, I’ve met and have worked with security researchers who are as young as 15.

The industry is incredibly supportive and rich on resources for self-paced learning. By working collaboratively on sourcing and reporting vulnerabilities, a new security researcher can find mentorship, build their network and learn by doing alongside masters in the space. There’s nothing else like this in the world.

**Related: Prioritize Cybersecurity to Protect Your Business Before It Is Too Late**

## Code wanted, credentials not needed.

Cybersecurity further democratizes access to high paid and high skill tech work because top talent isn't identified by their degrees or prestigious schools, just by the work that they've done.

This is the power of bug bounty programs. Anyone can start and build a portfolio of work that lets them apply for high paid tech jobs. My company also believes in this – we don't even look at college degrees or credentials. Our focus is on looking at your source code and hunger for knowledge.

**Related: Five Ways To Protect Your Company Against Cyber Attacks**

## Talent is global. Hire accordingly.

A better understanding of how to leverage the global accessibility of the cybersecurity industry can help solve the current talent gap.

According to the 2020 Cybersecurity Workforce, the industry currently needs about 3 million qualified cybersecurity workers. And 64% of the cybersecurity professionals surveyed say their organization is impacted by this skills shortage.

This talent gap is in part the result of hiring teams clinging to irrelevant credential requirements and not fully appreciating how to best harness the way that "bug bounty programs" allow teams unrivalled access to some of the world's top talent. A well-run bug bounty program can bridge this skills and opportunity gap and create a win-win by helping companies access top global security talent and top global talent to showcase across the ecosystem.

There’s a common saying that talent is equally distributed but opportunity is not. I often think of my old classmates and friends in Egypt who are incredibly technically talented but just didn’t have the access to the opportunities to build and develop these skills. Now that the Covid-19 pandemic has accelerated the move to remote and distributed teams, organizations should actively frame their cybersecurity recruiting strategies to be agnostic to geography and location and traditional credentials. This will enable them to recruit talented individuals and create new pathways into the industry.

**Related: One Shockingly Common Blind Spot that Can Derail Your Company’s Cybersecurity**

https://www.entrepreneur.com/article/369918