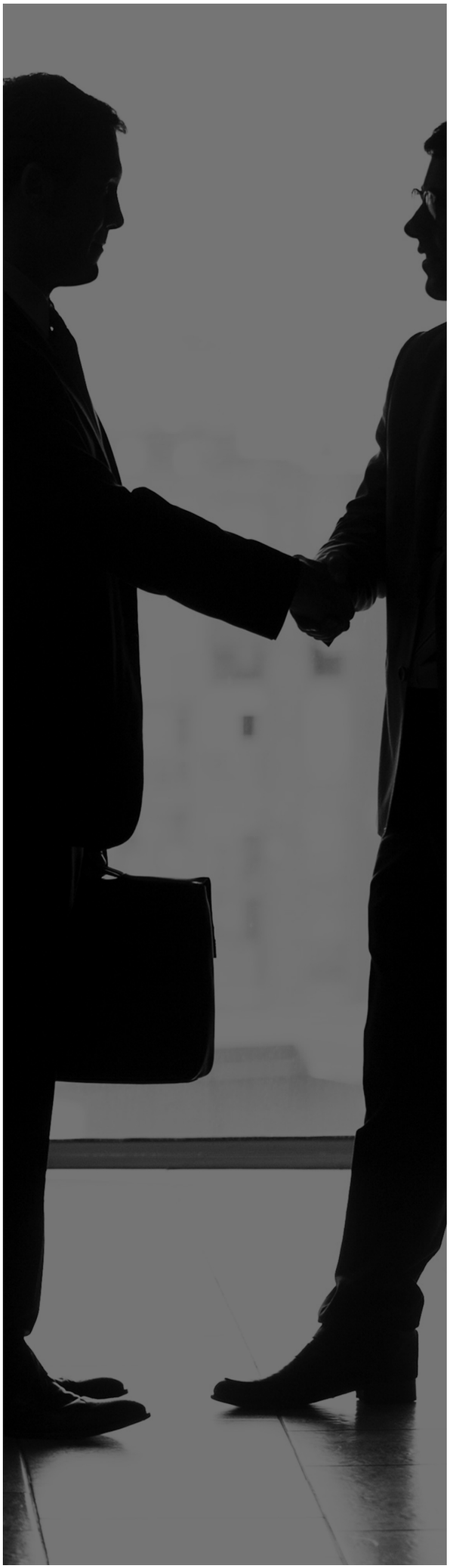

HERJAVEC GROUP

Cybersecurity Jobs Report

2018-2021 Edition

A Special Report from the Editors at Cybersecurity Ventures

Sponsored by Herjavec Group

Cybersecurity Ventures predicts there will be 3.5 million cybersecurity job openings by 2021.

Cybercrime will more than triple the number of job openings over the next 5 years.

Cybersecurity Ventures has reviewed and synthesized dozens of employment figures from the media, analysts, job boards, vendors, governments, and organizations globally, towards predicting the number of cybersecurity job openings over the next 5 years.

We predict there will be 3.5 million unfilled cybersecurity positions by 2021.

The cybersecurity job forecasts have been unable to keep pace with the dramatic rise in cybercrime, which is predicted to cost the world $6 trillion annually by 2021, up from $3 trillion in 2015.

The 2014 Cisco Annual Security Report ventured what became a widely popular cybersecurity jobs forecast over the past 3 years, originally stating "It's estimated that by 2014, the industry will still be short more than a million security professionals across the globe."

In 2015, Symantec expected the demand for cybersecurity talent would rise to 6 million globally by 2019, with a projected shortfall of 1.5 million.

> **"Despite having the largest information technology talent pool in the world, India is highly unlikely to produce an adequate number of professionals to close the cybersecurity skills gap."**

A 2016 skills gap analysis from ISACA estimated a global shortage of 2 million cybersecurity professionals by 2019 (a half-million more than Symantec's prior estimate), according to the UK House of Lords Digital Skills Committee.

The National Association of Software and Services Companies (NASSCOM) recently estimated that India alone will need 1 million cybersecurity professionals by 2020 to meet the demands of its rapidly growing economy.

Demand for security professionals in India will increase in all sectors due to the unprecedented rise in the number of cyberattacks, according to NASSCOM. Despite having the largest information technology talent pool in the world, India is highly unlikely to produce an adequate number of professionals to close the cybersecurity skills gap.

Israel — the world's second largest exporter of cybersecurity technology behind the U.S. — leads employer demand for cybersecurity talent by a wide margin, according to a 2016 report from Indeed, one of the world's largest job sites, with over 200 million unique visitors every month from over 60 different countries.

An Indeed blog states that Israel's strong showing is likely due in part to the emphasis the country places upon security. Veterans of the IDF's (Israel Defense Forces) elite cybersecurity Unit 8200 have founded many cybersecurity firms valued at hundreds of millions of dollars (or billions, according to other sources).

Intel Corp. conducted an eight-nation (Israel, the US, Australia, France, Germany, Japan, the UK and Mexico) survey on cybersecurity which concluded a global shortage of cybersecurity professionals in each country. In Israel 80 percent of those interviewed reported a shortage of workers.

In 2017 the U.S. employs nearly 780,000 people in cybersecurity positions, with approximately 350,000 current cybersecurity openings, according to CyberSeek, a project supported by the National Initiative for Cybersecurity Education (NICE), a program of the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce.

The current number of U.S. cybersecurity job openings is up from 209,000 in 2015. At that time, job postings were already up 74 percent over the previous five years, according to a Peninsula Press analysis of numbers from the Bureau of Labor Statistics.

"Until we can rectify the quality of education and training that our new cyber experts receive, we will continue to be outpaced by the Black Hats."

–Robert Herjavec, CEO and Founder of Herjavec Group

Robert Herjavec, Founder and CEO of Herjavec Group, a Managed Security Services Provider with offices and SOCs (Security Operations Centers) globally, says, "Unfortunately the pipeline of security talent isn't where it needs to be to help curb the cybercrime epidemic. Until we can rectify the quality of education and training that our new cyber experts receive, we will continue to be outpaced by the Black Hats."

Every IT position is also a cybersecurity position now. Every IT worker, every technology worker, needs to be involved with protecting and defending apps, data, devices, infrastructure, and people. The cybersecurity workforce shortage is even worse than what the jobs numbers suggest.

"I highly recommend pursuing your education in information technology or computer science" says Herjavec, directing his comments at IT workers and new entrants to the field — including college graduates. "There is a zero-percent unemployment rate in cybersecurity and the opportunities in this field are endless. Gone are the days of siloed IT and security teams. All IT professionals need to know security – full stop. Given the complexity of today's interconnected world, we all have to work together to support the protection of the enterprise."

Security starts at the top. Right now, about 65% of large U.S. companies have a CISO (Chief Information Security Officer) position, up from 50% in 2016, according to ISACA, an independent, nonprofit, global association.

Cybersecurity Ventures predicts that 100% of large companies globally will have a CISO position by 2021. They have to. The cybercrime and related workforce shortage is severe – and organizations need security leadership with a solid or dotted line to the CEO in order to remedy the problem.

The cybersecurity workforce shortage has left CISOs (Chief Information Security Officers) and corporate IT security teams shorthanded and scrambling for talent while the cyber attacks are intensifying.

Corporations are responding by placing some or all of their IT security into the hands of third parties. Last year, Microsoft estimated that 75 percent of infrastructure will be under third-party control (i.e., cloud providers or Internet Services Providers) by 2020. MSSPs (Managed Security Service Providers) are a subset of the third-parties, and they focus exclusively on security.

Outsourcing security introduces a whole new risk for enterprises — choosing the right third party which has the cyber defenders, cyber operations, and security platforms to effectively combat an increasingly hostile threatscape.

"Having a partnership with a third party Security Operations Center (SOC) provider is beneficial to companies that have limited IT resources and lack internal security expertise" says Melissa Zicopula, Vice President of Managed Security Services of Herjavec Group.

"I often explain to boards that Managed Security Services is the new house alarm" says Robert Herjavec. "The logs tell you if your house is safe. The insights SOCs can draw from data correlation will tell you if the other houses on the street are getting robbed. Security technology management keeps the system fine tuned. But the secret sauce? That's in data enrichment. That's where the magic happens."

"MSSPs need to continually evolve their practices because proactive threat detection and investigation is becoming the norm" adds Herjavec. "You can't just block and defend anymore. The role of the Threat Hunter is key as the expectation is that cyber operators not only detect but they investigate and analyze very sophisticated and persistent threats. Enterprises want to know where the threat originated, how they should respond and what can be done to contain the incident. Today, more often than not, we're seeing organizations turn to a third party for these answers."

While the third parties themselves have their work cut out for them in terms of recruiting security talent, they are in the best position to do so. MSSPs do some of the most cutting edge work in cyber, a big draw for the more talented candidates.

CISOs should think long and hard about how to engage with security outsourcers, and which ones to look at. MSSPs may be cybersecurity's saving grace.

HERJAVEC GROUP

About the Author

Steve Morgan is Founder and Editor-In-Chief at Cybersecurity Ventures. He oversees all of the editorial for Cybersecurity Ventures which includes our research, quarterly and annual reports, and directories.

About Cybersecurity Ventures

Cybersecurity Ventures is the world's leading researcher and publisher covering the global cyber economy. Our firm delivers cybersecurity market data, insights, and ground-breaking predictions to a global audience of CIOs and IT executives, CSOs and CISOs, information security practitioners, cybersecurity company founders and CEOs, venture capitalists, corporate investors, business and finance executives, HR professionals, and government cyber defense leaders.

For more information, visit http://www.cybersecurityventures.com/

About Herjavec Group

Dynamic entrepreneur Robert Herjavec founded Herjavec Group in 2003 to provide cybersecurity products and services to enterprise organizations. We have been recognized as one of the world's most innovative cybersecurity operations leaders, and excel in complex, multi-technology environments. Our service expertise includes Advisory Services, Technology Architecture & Implementation, Identity Services, Managed Security Services, Threat Management and Incident Response. Herjavec Group has offices and Security Operations Centers across the United States, United Kingdom and Canada.

For more information, visit **www.herjavecgroup.com.**

Follow Us
Herjavec Group
@HerjavecGroup