

Click to print or Select 'Print' in your browser menu to print this document.

Page printed from: <https://www.law.com/njlawjournal/2019/11/25/thinking-outside-the-box-u-s-immigration-options-for-cybersecurity-experts/>

# Thinking Outside the Box: U.S. Immigration Options for Cybersecurity Experts

Our nation is in dire need of experts who possess the advanced knowledge, skills and experience required to combat cybersecurity crimes; there is currently a shortage of U.S. workers who have these qualities,

By **Scott R. Malyk and Lin R. Walker** | November 25, 2019



shutterstock

Very few people would make a connection between cybersecurity and U.S. immigration law. In fact, a decade ago, very few people outside of the information technology (IT) industry knew what cybersecurity was or even considered it something worth worrying about. Many of us naively believed that with the right passwords, encryption software and firewalls, our data and information would be secure.

In recent years, however, our world has become far more technologically advanced and, as a consequence, technologically dependent. Nearly every occupation and industry has developed some use for artificial intelligence, a big data platform, or web-based application, whether it is banking, retail, pharmaceutical, medical, legal or agricultural.

Today, we are experiencing a generational shift in computing, with nearly every company, small and large, seeking to move networks, servers, data warehouses and virtualization software functions and components to a cloud-based infrastructure. This is largely because of the realization, over time, by many companies, that their "data is gold." Thus, a company's adoption of cloud-based technology has become the first priority for most Chief Information Officers (CIOs) and, thus, the use of such technology has skyrocketed. With this major shift to cloud-based computing, it's no surprise that cyber vulnerabilities within cloud technology will also increase. So in addition to migrating to the cloud in order to provide innovative services that enhance business and drive transformations, CIOs must also be cognizant of the ever-growing cybersecurity threats to such Internet-based technologies.

While these advances in technology have made our lives easier in many respects, they have also created significant opportunities for individuals and organizations to use the same technology to commit cybercrimes. Although cybersecurity is neither a new or emerging field, there has been something of a collective epiphany in the United States regarding the essential and significant role it plays in our everyday lives, particularly since 2016. Since that time, there have been daily reports of cybersecurity crimes, ranging from denials of service, to hacks and breaches of personal, financial and confidential information, to election meddling. Some of the most noteworthy examples of these damaging crimes include data breaches at

Equifax in September 2017; Capital One Bank in March 2019; Facebook in April 2019; and American Medical Collection Agency (a third-party billing collections firm for LabCorp and Quest Diagnostics) in June 2019.

In addition to these hacks and breaches, the use of ransomware has dramatically increased as well. Ransomware is a type of cyberattack that encrypts a computer's files (and makes unavailable to the owner/user of such data), in which the owner/user of the data must pay the attacker a "ransom" often in bitcoin or some other untraceable cryptocurrency to release the files. Since 2013, more than 170 U.S. county-, city- and state-government systems have been attacked using ransomware, including at least 45 law enforcement offices.

The prevalence of cybersecurity crimes, and their significant impact, became abundantly clear in the wake of the 2016 Presidential election, which experienced malicious hackings and massive breaches of campaign voter data, including hacking of election systems. As our election and voting systems become more data-driven and electronic, our nation becomes more susceptible to such cyberattacks, which have and will continue to impact our voting practices and democratic norms.

In an effort to protect our financial, personal, medical, and otherwise confidential data, as well as our election systems, we need to continue to attract and employ the services of the most qualified cybersecurity experts from around the world. However, at present, there is a dire shortage of such qualified experts in the United States. On Jan. 10, 2019, Jon Oltsik, Chief Security Officer of Enterprise Strategy Group (ESG) and a world renowned cybersecurity expert wrote:

At the end of each year, ESG conducts a wide-ranging global survey of IT professionals, asking them about challenges, purchasing plans, strategies, etc. As part of this survey, respondents were asked to identify areas where their organization has a problematic shortage of skills.

*In 2018-2019, cybersecurity skills topped the list — 53 percent of survey respondents reported a problematic shortage of cybersecurity skills at their organization. IT architecture/planning skills came in second at 38 percent.*

The cybersecurity skills shortage is nothing new. Alarming, the cybersecurity skills deficit has held the top position in ESG's annual survey every year... Furthermore, the percentage of organizations reporting a problematic shortage of cybersecurity skills continues to increase.

\*\*\*\*

Now, people like me have been talking about the cybersecurity skills shortage for years, and there are a lot of worthwhile industry and academic programs in place to address this issue. Despite these efforts, however, research from ESG and others indicates that the *cybersecurity skills shortage is getting incrementally worse each year*. (Emphasis added.)

(<https://www.csoonline.com/article/3331983/the-cybersecurity-skills-shortage-is-getting-worse.html> (<https://www.csoonline.com/article/3331983/the-cybersecurity-skills-shortage-is-getting-worse.html>))

Our technology and data infrastructure need significant work to keep them safe from hacks, breaches and ransomware attacks, but there are simply not enough qualified professionals in the U.S. to fill this need. In this regard, our business leaders and corporations must be open to recruiting and retaining qualified foreign nationals who possess the requisite skills, education and expertise to perform these duties.

In addition to the standard-issue H-1B and L-1B visa classifications, there is a variety of immigration options available to U.S. employers who seek to hire foreign nationals with cybersecurity expertise. One of these options is the O-1A nonimmigrant classification for individuals of extraordinary ability in the sciences or business. This often overlooked nonimmigrant visa classification is available to a foreign national who can demonstrate a level of expertise among a small percentage who have risen to the top of the field. Individuals who have made original, documented contributions to the field, as evidenced by patents and/or publications, and have served as the judge of the work of others (journal reviewers/editors) or in essential/critical capacities can readily qualify for the O-1A visa classification.

Another option available, which leads to permanent resident status in the United States, is the National Interest Waiver (NIW) petition. NIW petitions are typically granted to those who have exceptional ability and whose employment in the United States would greatly benefit our nation. Cybersecurity has proven to be an endeavor that is in the national interest of the United States. Thus, individuals seeking a NIW can establish exceptional ability through documented evidence confirming that they possess at least a Master's degree in a specialized field of study related to cybersecurity; possess at least 10 years of full-time employment experience in the field of cybersecurity; are recognized for their achievements in cybersecurity; and have publications in the field.

It is clear from the daily reports of cybersecurity crimes, that our nation is in dire need of cybersecurity experts who possess the resources, advanced knowledge, skills and experience required to combat these crimes. In this regard, as there is currently a shortage of U.S. workers who possess these qualities, U.S. corporations and governmental agencies should consider thinking "outside the box" as it relates to these immigration options in order to attract and recruit foreign nationals with this expertise.

While there are many immigration options available for both temporary and permanent employment of cybersecurity experts, it is best to plan ahead and consult with an attorney in advance to identify which options best meet the goals of the U.S. employer, the foreign national and, most importantly, the national interests of our country.

**Scott R. Malyk** and **Lin R. Walker** are attorneys with *Meyner and Landis LLP's Immigration Law Group*, specializing in all aspects of corporate and business-related U.S. immigration law.