CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

eMAGAZINE

IN THIS EDITION

NOVEMBER 2019

MORE INSIDE!

@MILIEFSKY

From the
Publisher...

New CyberDefenseMagazine.com website, plus updates at CyberDefenseTV.com & CyberDefenseRadio.com

Dear Friends,

Can you believe it's November 2019, already? We're almost into 2020 but we still have so much to accomplish this year – we have a new platform going live by December so stay tuned. Don't miss us at the InfoSecurity North America show in New York City November 20-21, 2019 https://www.infosecuritynorthamerica.com/ before we turn the corner into an early RSA Conference 2020 in late February, in San Francisco, CA, USA.

Our 8th annual InfoSec Awards for 2020 are now open and we hope to find more winners this year who are market leaders, innovators and those offering some of the best solutions for cyber security in the global marketplace. For those women who did not make our Top 25 Women in Cybersecurity for 2019 or missed out on the deadline, we have added Women in Cybersecurity as a new category this year. If you're an infosec innovator, please consider applying at: https://www.cyberdefenseawards.com/

We offer our own statistics that you are free to reuse anytime, from this page: http://www.cyberdefensemagazine.com/quotables/. We have many new interviews going live on https://www.cyberdefensetv.com and https://www.cyberdefenseradio.com this month, so please check them out and share links to them with your friends and co-workers. Let's all keep on innovating and finding ways to get one step ahead of the next threat!

Warmest regards,

Gary S. Miliefsky

Gary S.Miliefsky, CISSP®, fmDHS
CEO, Cyber Defense Media Group
Publisher, Cyber Defense Magazine

P.S. When you share a story or an article or information about CDM, please use #CDM and @CyberDefenseMag and @Miliefsky – it helps spread the word about our free resources even more quickly.

InfoSec Knowledge is Power. We will always strive to provide the latest, most up to date FREE InfoSec information.

From the Editor's Desk…

Turning a corner as leaves turn colors, changes are coming. Some of the biggest attack vectors we're predicting for 2020 include:

- Nation State Cyberespionage and Cyberwarfare
- Supply Chain Management Exploitation
- Cloud-based Identity Attacks
- New Deep Fake Spear Phishing Attacks
- Mobile Devices Become the Ultimate Backdoor
- IoT Devices Become New Critical Targets
- Ransomware will continue to escalate

….and we expect much more…so please keep reading, keep sharing and watch for the latest exploits as well as the best defenses to get one step ahead of the next threat, only here, at Cyber Defense Magazine.

Thank you so much!

To our faithful readers,

Pierluigi Paganini

Editor-in-Chief

@CYBERDEFENSEMAG

CYBER DEFENSE eMAGAZINE

Published monthly by the team at Cyber Defense Media Group and distributed electronically via opt-in Email, HTML, PDF and Online Flipbook formats.

PRESIDENT & CO-FOUNDER
Stevin Miliefsky
stevinv@cyberdefensemagazine.com

EDITOR-IN-CHIEF & CO-FOUNDER
Pierluigi Paganini, CEH
Pierluigi.paganini@cyberdefensemagazine.com

EDITOR-AT-LARGE & CYBERSECURITY JOURNALIST
Yan Ross, JD
Yan.Ross@cyberdefensemediagroup.com

ADVERTISING
Marketing Team
marketing@cyberdefensemagazine.com

CONTACT US:
Cyber Defense Magazine
Toll Free: 1-833-844-9468
International: +1-603-280-4451
SKYPE: cyber.defense

http://www.cyberdefensemagazine.com

PUBLISHER

Gary S. Miliefsky, CISSP®

Learn more about our founder & publisher at:
http://www.cyberdefensemagazine.com/about-our-founder/

WE'RE TURNING A CORNER INTO
8 YEARS OF EXCELLENCE!

Providing free information, best practices, tips and techniques on cybersecurity since 2012, Cyber Defense magazine is your go-to-source for Information Security. We're a proud division of Cyber Defense Media Group:

CYBERDEFENSEMEDIAGROUP.COM

MAGAZINE TV RADIO AWARDS

Secure Data Is Gold: U.S. Immigration Options for Cybersecurity Experts

By Lin Rose Walker, Esq. and Scott R. Malyk, Esq.

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 uses for data, whether it be used for artificial intelligence, machine learning, CRM or other applications, whether it is banking, retail, pharmaceutical, medical, oil &gas, agricultural or elsewhere.

Because the collection, processing and use of data has become such a valuable asset for so many companies and industries, 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. Indeed, a company's adoption of cloud-based technology, with appropriate safeguards, has become first priority for most Chief Information Officers (CIOs), thus, skyrocketing the use for cloud technology.

With this major shift to cloud-based computing, it's no surprise that cyber vulnerabilities within cloud technology are also on the rise. 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 cloud-based technologies.

While these advances in data and 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:

- September 2017 – Equifax announced a data breach that exposed the personal information of 147 million people in the United States;

- March 2019 – Capital One Bank experienced a data breach that exposed the personal information of nearly 106 million of the bank's customers and credit card applicants;

- April 2019 – Facebook experienced a data breach that exposed 540 million user records on Amazon's cloud computing service; and

- June 2019 – American Medical Collection Agency, a third-party billing collections firm which provides services for LabCorp and Quest Diagnostics experienced a data breach in which the personal, financial and medical data of 7.7 million LabCorp patients and 12 million Quest Diagnostics patients were disclosed.

- August 2019 – Twitter CEO Jack Dorsey's Twitter account was hacked on August 30 by a group that calls itself the Chuckle Squad. The hackers tweeted racial slurs, antisemitic messages and at least one Holocaust denial from Dorsey's account.

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. (https://www.cnn.com/2019/05/10/politics/ransomware-attacks-us-cities/index.html) Most recently, on August 20th, the State of Texas reported that twenty-three (23) towns

were struck by a coordinated ransomware attack. (https://www.cnbc.com/2019/08/19/alarm-in-texas-as-23-towns-hit-by-coordinated-ransomware-attack.html)

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. (https://cdt.org/issue/internet-architecture/election-cybersecurity/) 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. (https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/07/15/the-cybersecurity-202-here-s-an-overlooked-election-cybersecurity-danger-outdated-software/5d2bc0321ad2e552a21d53d4/)

In an effort to protect our financial, personal, medical, and otherwise confidential or personal 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 January 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. Alarmingly, 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)

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 are 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 ten (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 and 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 U.S. employer, the foreign national and most importantly, the national interests of our country.

About the Authors

Lin R. Walker and Scott R. Malyk are attorneys with Meyner and Landis LLP's Immigration Law Group, specializing in all aspects of corporate and business-related US immigration law. Walker and Malyk represent a diverse group of corporate and individual clients in a variety of industries, with a special emphasis on researchers, developers, architects, engineers, data scientists and business people in the high tech industry nationwide, which includes individuals whose work is in the national interest of the United States.