CYBERSECURITY

advisory

HELP WANTED: SHORTAGE OF CYBERSECURITY EXPERTS POSES CHALLENGES AND RISKS

If I was a parent of a first-year college student who was undecided in what major to declare, I'd firmly nudge him or her to consider going into nursing/healthcare studies or computer science/programming. Given the poor state of our global health and rapidly increasing cybersecurity risks and growth of artificial intelligence, both of these fields have limitless opportunities and growth potential. Indeed, a 2019 cybersecurity workforce study by the International Information System Security Certification Consortium (ISC^2) concluded that a "shortage in the global cybersecurity workforce continues to be a problem for companies in all industries and of all sizes." In the United States, for example, there is a shortage of 500,000 cybersecurity workers. To meet this demand, the United States cybersecurity workforce would need to grow by 62% and the global cybersecurity workforce needs to expand by 145%.

This lack of qualified talent is the top concern among cybersecurity professionals. This gap exposes governments and businesses to substantial risks as threats from bad actors continue to grow. Although it is not clear why this gap has grown so large and quickly, there are several theories behind this phenomenon:

- It's possible that the pace of technological advancement in cybersecurity and computer systems is simply outpacing the human capital available to service these critical functions. As systems become more robust and sophisticated, this creates tremendous demands on the need to service them and stay up to date. This results in human capital consistently trying to play "catch-up" to the ever-increasing and expanding nature of cybersecurity systems. This deficit is also likely compounded by the relative lack of women traditionally interested in cybersecurity careers. As ISC^2 notes in its study, cybersecurity professionals are twice as likely to be male.
- Cybersecurity jobs are generally not high-profile and are rarely touted in the press as important or critical. Often management and executives either do not fully understand or value the critical role that cybersecurity professionals play in protecting infrastructure. Cybersecurity professionals quietly toil away in front of screens and in server rooms, not on an organization's front lines. Despite this critical importance, they generally lack visibility and acknowledgment in organizations due to the nature of their jobs. A good day for a cybersecurity professional is when nothing bad happens.
- Information technology/security has often been outsourced to outside vendors and IT firms. However, businesses of all sizes are beginning to recognize the need and importance of having in-house IT and cybersecurity. Therefore, businesses are beginning to recruit, train, and retain their own talent. This shift toward a more in-house model has resulted in a sharp demand which the current workforce cannot meet.

PANNONE LOPES
DEVEREAUX & O'GARA LLC
counselors at law

So, what do we do to address this workforce gap? First, we should continue to encourage girls and women to explore education and career opportunities in STEM and computer science. This will serve two important goals: it would expand the pool of available talent interested in cybersecurity and it would diversify a workforce that has traditionally been viewed as male-dominant.

Second, ISC2 recommends that businesses ensure that they appeal to cybersecurity professionals. This includes valuing IT/cybersecurity professionals and giving them management (not just service) roles, highlighting the opportunities for growth within the organization, and paying for needed or desired cybersecurity certifications. And, organizations should recognize the critical importance of these professionals by paying market rates for talent. (ISC^2 notes that the average North American cybersecurity professional earned $91,000 in 2019.)

Next, ISC^2 suggests that organizations consider hiring recent college graduates for basic or entry-level positions who lack cybersecurity certifications. Instead, these workers could then obtain any necessary certifications while they grow and learn on the job. This would expand the pool of available talent and create an organizational culture of growth, loyalty, and advancement from within. Companies should therefore be cautious when drafting job descriptions and be thoughtful as to whether specific certifications are really needed to perform entry- or low-level job tasks.

Finally, organizations should still continue to recruit from within when appropriate. As ISC^2 notes, many human resource, legal, and finance professionals have transferable skills (such as problem-solving and crisis management) that would lend themselves well to a cybersecurity role. As these traditional in-house functions are commoditized or outsourced overseas, companies could use this dynamic to their advantage by retaining and repurposing talented in-house workers who may be interested in a career change or new challenge.

For more information, please contact PLDO Partner Brian J. Lamoureux at bjl@pldolaw.com or 401-824-5155. Attorney Lamoureux is a member of the firm's litigation, corporate, and cybersecurity teams.

Brian J. Lamoureux
Partner

PANNONE LOPES
DEVEREAUX & O'GARA LLC
counselors at law

This memorandum is intended to provide general information of potential interest to clients and others. It does not constitute legal advice. The receipt of this memorandum by any party who is not a current client of Pannone Lopes Devereaux & O'Gara LLC does not create an attorney-client relationship between the recipient and the firm. Under certain circumstances, this memorandum may constitute advertising under the Rules of the Massachusetts Supreme Judicial Court and the bar associations of other states. To insure compliance with IRS Regulations, we hereby inform you that any U.S. tax advice contained in this communication is not intended or written to be used and cannot be used for the purpose of avoiding penalties under the Internal Revenue Code or promoting, marketing or recommending to another party any transaction or matter addressed in this communication.