Global study reveals businesses and countries vulnerable to shortage of cybersecurity talent

27 July 2016

Intel Security, in partnership with the Center for Strategic and International Studies (CSIS), has just released Hacking the Skills Shortage, a global report outlining the talent shortage crisis impacting the cybersecurity industry across both companies and nations. A majority of respondents (82 percent) admit to a shortage of cybersecurity skills, with 71 percent of respondents citing this shortage as responsible for direct and measurable damage to organizations whose lack of talent makes them more desirable hacking targets.

"A shortage of people with cybersecurity skills results in direct damage to companies, including the loss of proprietary data and IP," said James A Lewis, senior vice president and director of the Strategic Technologies Program at CSIS. "This is a global problem; a majority of respondents in all countries surveyed could link their workforce shortage to damage to their organization."

In 2015, 209,000 cybersecurity jobs went unfilled1 in the United States alone. Despite 1 in 4 respondents confirming their organizations have lost proprietary data as a result of their cybersecurity skills gap, there are no signs of this workforce shortage abating in the near-term. Respondents surveyed estimate an average of 15 percent of cybersecurity positions in their company will go unfilled by 2020. With the increase in cloud, mobile computing and the Internet of Things, as well as advanced targeted cyberattacks and cyberterrorism across the globe, the need for a stronger cybersecurity workforce is critical.

"The security industry has talked at length about how to address the storm of hacks and breaches, but government and the private sector haven't brought enough urgency to solving the cybersecurity talent shortage," said Chris Young, senior vice president and general manager of Intel Security Group. "To address this workforce crisis, we need to foster new education models, accelerate the availability of training opportunities, and we need to deliver deeper automation so that talent is put to its best use on the front line. Finally, we absolutely must diversify our ranks."

The demand for cybersecurity professionals is outpacing the supply of qualified workers, with highly technical skills the most in need across all countries surveyed. In fact, skills such as intrusion detection, secure software development and attack mitigation were found to be far more valued than softer skills including collaboration, leadership and effective communication.

This report studies four dimensions that comprise the cybersecurity talent shortage, which include:

1. Cybersecurity Spending: The size and growth of cybersecurity budgets reveals how countries and companies prioritize cybersecurity. Unsurprisingly, countries and industry sectors that spend more on cybersecurity are better placed to deal with the workforce shortage, which according to 71 percent of respondents, has resulted in direct and measureable damage to their organization's security networks.
2. Education and Training: Only 23 percent of respondents say education programs are preparing students to enter the industry. This report reveals non-traditional methods of practical learning, such as hands-on training, gaming and technology exercises and hackathons, may be a more effective way to acquire and grow cybersecurity skills. More than half of respondents believe that the cybersecurity skills shortage is worse than talent deficits in other IT professions, placing an emphasis on

continuous education and training opportunities.

3. Employer Dynamics: While salary is unsurprisingly the top motivating factor in recruitment, other incentives are important in recruiting and retaining top talent, such as training, growth opportunities and reputation of the employer's IT department. Almost half of respondents cite lack of training or qualification sponsorship as common reasons for talent departure.
4. Government Policies: More than three-quarters (76 percent) of respondents say their governments are not investing enough in building cybersecurity talent. This shortage has become a prominent political issue as heads of state in the U.S., U.K., Israel and Australia have called for increased support for the cybersecurity workforce in the last year.

Recommendations for Moving Forward:

- Redefine minimum credentials for entry-level cybersecurity jobs: accept non-traditional sources of education
- Diversify the cybersecurity field
- Provide more opportunities for external training
- Identify technology that can provide intelligent security automation
- Collect attack data and develop better metrics to quickly identify threats

More information: or more information on these findings, along with Intel Security's proposed recommendations, read the full report: Hacking the Skills Shortage: A study of the international shortage in cybersecurity skills: mcafee.com/skillsshortage

Provided by Intel