Executive Summary

Hacking the Skills Shortage

A study of the international shortage in cybersecurity skills

The global shortage of trained and qualified cybersecurity talent exacerbates the already challenging task of defending against the rapidly accelerating volume of sophisticated advanced threats. The Center for Strategic and International Studies (CSIS) performed a study to quantify the cybersecurity workforce shortage across eight countries (Australia, France, Germany, Israel, Japan, Mexico, the UK, and the US). Information technology (IT) decision makers in both the public and private sectors were surveyed, with the focus on four key areas of cybersecurity workforce development: security spend, educational programs, employer dynamics, and public policies. The study offers valuable information that can help companies and governments build a more robust and sustainable cybersecurity workforce with the needed skills. It also offers multiple concrete recommendations on how to improve the current cybersecurity talent deficit and enhance overall global cybersecurity.

Key Findings

- The cybersecurity talent shortage is widespread. According to the CSIS study, 82% of participants report a shortage of cybersecurity skills in their organizations. The low supply and high demand for cybersecurity professionals has also driven up salaries. In the US, cybersecurity positions pay almost 10% more than other IT jobs.
- The talent shortfall makes organizations more vulnerable to attackers. Seventy-one percent of respondents support this idea. One in four say that lack of sufficient cybersecurity staff has actually contributed to data loss or theft and reputational damage.
- Certain skills are in high demand. The most desirable skills cited in all eight countries are intrusion detection, secure software development, and attack mitigation.

- Hands-on training is the best way to acquire cybersecurity skills. While approximately 50% of decision makers surveyed prefer a bachelor's degree in a relevant technical discipline as the minimum entry-level job requirement, most respondents believe that experience, hacking competitions, and professional certifications are better ways to acquire cybersecurity skills than is earning a degree.
- Technology can help compensate for the talent shortage. About nine out of 10 respondents said that security technology could help fill in the gaps, and 55% believe that, five years from now, cybersecurity solutions will be sufficiently advanced to meet their organization's needs. They are also outsourcing security functions and processes that lend themselves to automation.
- Governments are not investing enough in cybersecurity. Seventy-six percent of respondents say their governments are not investing enough in programs to help cultivate cybersecurity talent and believe that the laws and regulations for cybersecurity in their country are inadequate.

Four Dimensions of the Cybersecurity Workforce Shortage

Cybersecurity spending

It is estimated that total global cybersecurity spending will be more than $100 billion over the next four to five years.[1] The biggest spenders and consumers of cybersecurity technology and services are the US government and the financial services industry, which are prime targets for attackers. By investing heavily in cybersecurity, these two sectors are better equipped to deal with the workforce shortage issue and can help drive best practices for training and hiring.

Education and training

As the CSIS report points out, while academic degrees may be a minimal prerequisite for cybersecurity positions, most decision makers believe that hands-on experiential learning is the best training for these jobs—only 23% of respondents say education programs are preparing students to enter the industry. According to the study, the US and UK rank highest in current investment in cybersecurity education, while Mexico, France, and Japan rank lowest. More than three-fourths of survey respondents cite professional certifications as an effective way to demonstrate skills. And two in five say that hacking competitions are the best way to gain skills.

Employer dynamics

What are the top recruitment strategies for attracting and retaining cybersecurity professionals? Salary tops the list followed by training, IT department reputation, and advancement opportunities. Nearly 50% of survey participants say that lack of training or sponsorship for certification programs are common reasons for employees leaving a company. Since it often takes time to develop a strong cybersecurity staff, organizations are turning to technology to fill in the gaps. Approximately nine out of 10 respondents say technological advancements in cybersecurity could compensate for the workforce skills gap. In addition, outsourcing certain security functions, such as risk assessment and mitigation, network monitoring and access management, and repair of compromised systems, is also a widely accepted alternative. More than 60% of survey respondents outsource at least some aspect of their cybersecurity workload.

Government policies

Many countries, including the US, UK, Israel, and Australia, are increasing support for the cybersecurity workforce issue. Most countries also have legislation specific to enhancing cybersecurity education, but more than 75% of survey respondents say their governments are not investing enough in building cybersecurity talent, and the same percentage said the laws and regulations for cybersecurity in their country are insufficient.

Recommendations

Redefine minimum credentials for entry-level cybersecurity jobs and accept non-traditional sources of education

Because so few universities and colleges across all countries offer cybersecurity concentrations, the CSIS data would suggest that hiring managers need to value professional certifications and hands-on experience over degrees. Universities and high schools should start offering this type of practical cybersecurity training to help talented individuals hone their skills. These kinds of programs present an opportunity for governments, the private sector, and educational institutions to work together toward enhancing curricula and provide internships and training opportunities.

Diversify the cybersecurity field

According to a number of studies, women and minorities are underrepresented in this field. Additionally, rigid immigration policies shrink the pool of high-skilled workers critical to the cybersecurity workforce. The cybersecurity workforce can be rapidly expanded in the United States and other countries with similar immigration conditions by increasing the number of work visas and by including minorities and women. Another barrier to increasing the cybersecurity workforce is the stigma associated with people who have hacking experience. Employers need to develop a more flexible attitude toward hiring people who have been involved with hacking, as they have extremely valuable insights and skills.

Provide more opportunities for external training

Ongoing training programs are vital to retaining cybersecurity talent, as the lack of such programs often causes people to seek employment elsewhere. Governments and the private sector should collaborate on ways to enhance training opportunities for both students and current employees who want to improve their skills.

Evolve skills for automation

The CSIS survey reveals that organizations are looking to automate cybersecurity functions to offset the skills shortage, which means that the cybersecurity workforce will be compelled to adapt its skills to these new processes. As automation creates operational efficiencies, cybersecurity professionals will focus more of their time and effort on detecting, analyzing, and remediating more advanced threats.

Collect data and develop better metrics

By gathering data on the cybersecurity labor market and standardized job functions, the private sector, government, and education can develop a common taxonomy of clearly defined high-value cybersecurity skills that apply across all industry sectors.

Conclusion

A robust workforce is essential for effective security—more so today than ever before. The global cybersecurity talent shortage can be addressed by bringing more talented individuals into this profession through improvements in education, workforce diversity, training opportunities, security technology, and data collection.

Visit **mcafee.com/skillsshortage** to read the full report.

[1] http://www.forbes.com/sites/stevemorgan/2016/02/12/cybersecurity-market-outlook-for-2016-to-2020/#185c567a74a4

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com