McAfee
Together is power.

Hacking the Skills Shortage

A focus on the cybersecurity skills shortage in Financial Services and Insurance

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. This executive summary focuses on the answers given by respondents within the financial services and insurance sectors, but includes comparisons and references to the data overall. The cross sector report is also available.

Connect With Us

Key Findings

- The cybersecurity talent shortage is widespread. According to the CSIS study, 81% of the financial services sector report a shortage of cybersecurity skills in their organizations. The low supply and high demand for cybersecurity professionals has also driven up salaries. In financial services, cybersecurity positions pay around 11% more than the overall average. On top of this, in the US, cybersecurity as a whole pays almost 10% more than other IT jobs. These two factors indicate that cybersecurity professionals in financial services are earning, on average, 22% more than their other IT function peers in other sectors.
- The talent shortfall makes organizations more vulnerable to attackers. Seventy-four percent of financial services respondents support this idea, compared to 71% of respondents from all sectors. One in four say that lack of sufficient cybersecurity staff has actually contributed to loss of proprietary data, and one in three say that it has made them desirable hacking targets.
- Certain skills are in higher demand in financial services than in other sectors, although they follow the same trend. In priority order, these are secure software development (+6% on cross-sector average), intrusion detection (+2%), and attack mitigation (+2%).
- While all sectors overall agree that hands-on experience is the best way to acquire cybersecurity skills, the financial services sector values professional certifications and both bachelor's and master's degrees more than the average.
- Technology can help compensate for the talent shortage, although the financial services sector differs in opinion from other industries. Only 35% compared to a survey average of 47% believe that technology can fully- or over-compensate for the skills shortage, but 50% compared to a survey average of 42% believe that it can "somewhat compensate." However, 62% compared to a survey average of 55% believe that cybersecurity solutions will be sufficiently advanced to meet the majority of their organization's needs in five years' time. They are also outsourcing security functions and processes that lend themselves to automation, particularly in the area of detecting threats.
- Governments are not investing enough in cybersecurity. Seventy-five percent of financial services respondents say their governments are not investing enough in programs to help cultivate cybersecurity talent and 70% believe that the laws and regulations for cybersecurity in the financial services sector 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 25% of financial services respondents say education programs are preparing students to enter the industry. Seventy-seven percent of financial services 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 across the board and is valued even more highly in the financial services sector. Following that is the level of training offered and the reputation of the IT department, with financial services showing little difference of opinion with other sectors overall, although being sponsored to study and innovation appear to play a more important role. Headhunting appears to be more active in financial services than other sectors, with 4% more respondents saying that people leave due to being recruited by prior team mates having gone to other companies, compared to the overall average. The skills gap in financial services could be filled with technological advancements in cybersecurity or by outsourcing, with 69% of financial services respondents saying their organization outsources some, all, or most of their cybersecurity compared to a cross-sector average of 63%. Commonly outsourced functions include risk assessment and mitigation, network monitoring and access management, and repair of compromised systems.

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 76% 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. This may be trickier to achieve in the financial services sector than in others, due to a long legacy of graduate-hiring schemes; however, this could represent an opportunity to work together with educational institutions and the government to enhance curricula and provide internships and other 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. The financial services sector values skills such as those acquired in hacking contests more highly than other sectors, although respondents were slightly less likely to have taken part in one than respondents in other sectors (49% versus 51%, respectively). Staff could be encouraged and sponsored to enter these national and international events to sharpen their cybersecurity 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, a collaborative approach between the private and public sectors could develop a common taxonomy of clearly defined high-value cybersecurity skills that apply across all industry sectors.

Conclusion

The financial services sector, while paying salaries on average 22% higher than other IT functions, cannot rely on this alone to attract and retain cybersecurity professionals. With high stakes at play for the sector as a whole, innovation and automation must play a part in the future of cybersecurity.

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

Learn More

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

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com