Cybersecurity Skills Crisis Continues for Fifth Year, Perpetuated by Lack of Business Investment

Annual global study from ESG and ISSA reveals not offering competitive compensation as the top factor contributing to the skills shortage for respondents' organizations

Vienna, VA, July 28, 2021 - The cybersecurity skills crisis continues on a downward, multi-year trend of bad to worse and has impacted more than half (57%) of organizations, as revealed today in the fifth annual global study of cybersecurity professionals by the Information Systems Security Association (ISSA) and industry analyst firm Enterprise Strategy Group (ESG). This annual study seeks to understand the perspectives of the people on the information security career path to help others understand the challenges of this important field.

The new research report, *The Life and Times of Cybersecurity Professionals 2021*, surveyed 489 cybersecurity professionals and reveals several nuances surrounding the well-documented cybersecurity skills shortage. The top ramifications of the skills shortage include an increasing workload for the cybersecurity team (62%), unfilled open job requisitions (38%), and high burnout among staff (38%). Further, 95% of respondents state the cybersecurity skills shortage and its associated impacts have not improved over the past few years and 44% say it has only gotten worse.

Notably, the three most-often cited areas of significant cybersecurity skills shortages include cloud computing security, security analysis and investigations, and application security. These areas should be the focus for cybersecurity professionals when looking to develop skills.

The cybersecurity profession remains systemically undervalued

Businesses are not investing in their people in a manner that appropriately reflects the direness of today's cyberthreat landscape. A striking 59% of respondents said their organization could be doing more to address the cybersecurity skills shortage, with nearly one-third noting that their organization could be doing *much* more.

- **Cybersecurity professionals need fair and competitive compensation.** This came up several times in the research report and is clearly critical to hiring and retaining security personnel. In a new finding this year, not offering competitive compensation is the top factor (38%) contributing to the organizations' cyber skills shortage because it makes it difficult to recruit and hire the cybersecurity professionals that organizations need. More than three-quarters (76%) of organizations admit that it is difficult to recruit and hire cybersecurity staff, with nearly one-fifth (18%) stating it is extremely difficult. Being offered a higher compensation package is the main reason (33%) CISOs leave one organization for another.

- **Investments in cybersecurity training needs to be funded appropriately.** When asked what actions organizations could take to address the cybersecurity skills shortage, the biggest response (39%) was an increase in cybersecurity training so candidates can be properly trained for their roles. To maintain and advance their skill sets, many cybersecurity professionals seek to achieve at least 40 hours of training each year. Nearly a quarter (21%) of those surveyed did not meet 40 hours of training per year. The main reason they cited was that their jobs do not pay for 40 hours of training per year and they can't afford it by themselves, according to nearly half (48%) of respondents.

- **The cybersecurity training paradox continues and needs attention.** Nearly all (91%) respondents agree that cybersecurity professionals must keep up with their skills or the organizations they work for are at a significant disadvantage against today's cyber-adversaries. Despite this need, 59% state that while they try to keep up with cybersecurity skills development, job requirements often get in the way—the paradox that professionals face where they are called upon to make up for the existing skills shortage in addition to falling behind on their own development.

- **Human resources and cybersecurity teams need to align on business value.** Nearly one in three (29%) professionals surveyed said the HR departments at their organizations likely exclude strong job candidates because they don't understand the skills necessary to work in cybersecurity. One in four also said job postings at their organizations tend to be unrealistic, demanding too much experience, too many certifications, or too many specific technical skills. Nearly a third (30%) suggested CISOs try to better educate HR and recruiters on real-world cybersecurity goals and needs and 28% said job recruitments need to be more realistic with the typical levels of experience cybersecurity professionals have.

- **Business and cyber leaders need to work together to improve organizational dynamics.** Business executives must embrace cybersecurity as a core component of the business while CISOs need to move their people, processes, and technologies closer to the business. Organizations should be alarmed by the fact that:
    - 29% of respondents said the security team's relationship with HR is fair or poor.
    - 28% said the relationship with line-of-business managers is fair or poor.
    - 27% of respondents said that the relationship with the board of directors is fair or poor.
    - 24% said the relationship with the legal team is fair or poor.

"There is a lack of understanding between the cyber professional side and the business side of organizations that is exacerbating the cyber skills gap problem," said Candy Alexander, Board President, ISSA International. "Both sides need to re-evaluate the cybersecurity efforts to align with the organization's business goals to provide the value that a strong cybersecurity program brings towards achieving the goals of keeping the business running. Cybersecurity leaders should be able to link the security efforts directly to strategic business goals."

"This report reveals some deep-seated issues with cybersecurity professionals and their organizations," said Jon Oltsik, Senior Principal Analyst and ESG Fellow. "ESG and ISSA hope that cybersecurity professionals use this research to better understand their profession and peers as they manage their careers. For business and cybersecurity professionals, the data

should be seen as a set of guidelines for maximizing cybersecurity investment, improving cybersecurity job satisfaction, and aligning cybersecurity with the business mission. The message is clear: Organizations with a cybersecurity culture are in the best position."

After reviewing this data, ESG and ISSA recommend that cybersecurity professionals take a holistic approach of continuous cybersecurity education (starting early with public education), comprehensive career development, and career mapping/planning—all with the support and integration with the business.

The full report can be downloaded here.

About ISSA

The Information Systems Security Association (ISSA)™ is the community of choice for international cyber security professionals dedicated to advancing individual growth, managing technology risk, and protecting critical information and infrastructure. ISSA members and award winners include many of the industry's notable luminaries and represent a broad range of industries – from communications, education, healthcare, manufacturing, financial and consulting to IT – as well as federal, state and local government departments and agencies. Through regional chapter meetings, conferences, networking events and content, members tap into a wealth of shared knowledge and expertise. Follow us on Twitter at @ISSAINTL. Learn more about ISSA.

About ESG

Enterprise Strategy Group (ESG) is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community. It is increasingly recognized as one of the world's leading analyst firms in helping technology vendors make strategic decisions across their go-to-market programs through factual, peer-based research. ESG is a division of TechTarget, Inc. (Nasdaq: TTGT), the global leader in purchase intent-driven marketing and sales services focused on delivering business impact for enterprise technology companies.