Cybersecurity Skills Crisis Worsens for Fourth Year in a Row, Impacting 70% of Organizations

Fourth annual global study from ESG and ISSA finds 45% state cybersecurity skills shortage has only gotten worse over the past few years. Why has nothing changed?

Milford, MA and Vienna, VA, July 30, 2020 (BUSINESSWIRE) – The cybersecurity skills crisis continues to worsen for the fourth year in a row and has impacted nearly three quarters (70 percent) of organizations, as revealed today in the fourth annual global study of cybersecurity professionals by the Information Systems Security Association (ISSA) and independent industry analyst firm Enterprise Strategy Group (ESG). The top ramifications of the skills shortage for organizations (or cybersecurity teams) include an increasing workload, unfilled open job requisitions, and an inability to learn or use cybersecurity technologies to their full potential, putting organizations at significant risk.

The cybersecurity skills gap discussion has been going on for nearly 10 years. The study confirms that there has been no significant progress towards a solution to this problem during the four years it has been closely researched. In fact, 45 percent of respondents state the cybersecurity skills shortage and its associated impacts have only gotten worse over the past few years. The question that must be answered is then: Why has nothing changed for the better?

ISSA and ESG believe that the root cause has never been addressed. What's needed is a holistic approach of continuous cybersecurity education, where each stakeholder needs to play a role versus operating in silos. The data uncovered in this research year over year point to these indicators:

Cybersecurity professionals need a comprehensive globally accepted career development plan

Without guidance and a clear path to follow, it is difficult for new candidates to know what is needed and how to acquire the skills necessary to enter the profession. Current professionals are far too often left figuring out how to advance their careers on their own. The ESG/ISSA research reinforces these points as:

- **Cybersecurity professionals continue to need career guidance.** Sixty-eight percent of the cybersecurity professionals surveyed don't have a well-defined career path and historical solutions are only compounding problems.
- **Cybersecurity careers depend upon hands-on experience and hands-on experience requires a job.** When asked which was most important for their career development: hands-on experience or security certifications, 52 percent chose hands-on experience. Still, 44 percent claim that hands-on experience and certifications are equally important. This combination requires the right job, the right experience, and the right career plan but few cybersecurity professionals can claim this combination.
- **It takes years to become a proficient cybersecurity professional.** Thirty-nine percent believe it takes anywhere from 3 to 5 years to develop real cybersecurity proficiency, while 22 percent say 2 to 3 years and 18 percent claim it takes more than 5 years. This means that entry level cybersecurity pros should be viewed as long-term investments, not immediate problem solvers.

Businesses are not investing in their people or supporting cybersecurity integration within the organization

Sixty-four percent of respondents believe their organization should be doing somewhat or a lot more to address cybersecurity challenges. ESG and ISSA believe that business executives see this as a technical problem rather than a business issue.

- **Organizations are not providing the right level of cybersecurity training**. Thirty-six percent of respondents reported that they thought that their organizations should provide a bit more cybersecurity training, while 29 percent believe their organizations should provide significantly more training. Further, 28 percent believe they are not providing enough training for non-technical employees. Based on 4 years of research, training seems to be a perpetual shortcoming. Alarmingly, there seems to be on plan for improvement.
- **CISOs and business executives could do more together**. Fifty-five percent believe there is adequate CISO participation with executives and corporate boards in 2020, trending upward slightly. Still, 24% think that CISOs and business executives could do more together.

Other critical constituencies were also rated on their ability to keep up with cybersecurity challenges and the data indicates that industry and community at large need to step up: For example, 68 percent of respondents believe that **cybersecurity technology and service vendors** should be doing somewhat or a lot more and 71 percent of respondents believe the **cybersecurity community at large** should be doing somewhat or a lot more.

"The cybersecurity gap cannot be addressed by simply filling the pipeline with new people. What's needed is a holistic approach, starting with public education, comprehensive career development and planning, and career mapping – all with the support and integration with the business," said Candy Alexander, Board President, ISSA International.

"As this and past reports clearly indicate, key constituents are not looking at the profession strategically. While we are making some fragmented progress, the same issues present themselves year after year, including a shortage of skills, under-trained employees, and the stress and strain caused by a career in the cybersecurity field. These disturbing trends should be of concern to corporate directors and business executives, particularly in light of the alarming findings this year that 67% of respondents believe that cyber-adversaries have a big advantage over cyber-defenders," said Jon Oltsik, Senior Principal Analyst and ESG Fellow.

The full report, "The Life and Times of Cybersecurity Professionals 2020," represents 327 global security and IT professionals and contains much more research spanning the topics of cybersecurity careers; skills development; cybersecurity organizational considerations; security incidents and vulnerabilities; cybersecurity skills shortage; and cybersecurity activities. It 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 analyst, research, and strategy firm providing market intelligence and actionable insight to the global technology community. ESG is increasingly recognized as one of the world's leading and most influential independent analyst firms.