FOR IMMEDIATE RELEASE

# Cyber Security Skills Crisis Causing Rapidly Widening Business Problem

*Second annual global study from ESG and ISSA finds cyber security skills shortage worsening and impacting 70% of organization; business investing in the wrong places*

**Milford, MA and Reston, VA – November 8, 2017 –** Building on the conclusions of last year's groundbreaking global study of cyber security professionals, the Information Systems Security Association (ISSA) and independent industry analyst firm Enterprise Strategy Group (ESG) revealed today trending data finding that the cyber security skills shortage is worsening and becoming a rapidly widening business problem. The majority of survey respondents (70 percent) continue to believe that the cyber security skills shortage has had an impact on their organization - yet these same organizations (62 percent, up almost 10 percent from last year) are falling behind in providing an adequate level of training for their cyber security professionals.

Further, the report confirms that the cyber security skills shortage is exacerbating the number of data breaches: Forty-five percent of organizations experienced at least one security event over the past two years and 91 percent of survey respondents believe most organizations are vulnerable to a significant cyber-attack or data breach. The cyber security skills shortage represents the top two contributing factors to these security events, with the first being a lack of adequate training of non-technical employees (31 percent) and the second being a lack of adequate cyber security staff (22 percent). These are followed by business executive management making cyber security a low priority (20 percent).

Additionally, there continues to be acute shortages in key areas with little improvement from last year. Thirty-one percent (31 percent) of respondents point to a shortage of  security analysis & investigations skills, 31 percent indicate a shortage of application security skills, and 29 percent claim a shortage of cloud computing security skills.

ISSA and ESG believe that this study offers a warning to organizations, who are trying to defend against increasing threats and regulatory demands, with a cyber security team that is understaffed and lacking advanced skills.

"The cyber security skills shortage represents an existential threat to our national security and this year-over-year comparison data bears out this fact. We are not making progress, cyber security professionals can't scale, and the implications of the skills shortage are becoming more pervasive and ominous. It is clear that the solution must be about more than filling jobs. It is about creating an environment from the top down of cyber security as a priority," said Jon Oltsik, Senior Principal Analyst at the Enterprise Strategy Group (ESG) and the author of the report.

“The Life and Times of Cyber Security Professionals” in-depth report of 343 global cyber security professionals explores over 45 questions to better understand the staffing and skills shortage and identify impacts to business, IT and the threat landscape.

“While there are many studies on the cyber security workforce gap, this is the only one to identify and go after the root cause of the deepening cyber security skills gap and provide actionable steps that every organization can take. The findings are clear that, while organizations have been investing in new cyber security technology, they are not investing enough in their people. We, as a profession, need to help business understand the cyber security skills investment vs. risk tradeoff,” said Candy Alexander, member of the ISSA International Board of Directors and Chief Architect of the ISSA Cyber Security Career Lifecycle.

**Top Five Cyber Security Investment Mistakes and Fixes for Business:**

1. *Not Aligning Cyber Security and Business Goals*: Respondents suggest the number one most beneficial action organizations can take is adding goals and metrics to IT and business managers (43 percent) and vice versa.
2. *Not Building Repeatable Processes*: Survey respondents say one of the top two cyber security challenges is too many manual and informal processes for cyber security (28 percent). They suggest that the number two most beneficial action organizations can take is to document and formalize all cyber security processes (41 percent).
3. *Not Investing in Training*: Although companies are increasing their cyber security spend, especially in technology, they are investing in the wrong places. Survey respondents suggest that three of the most beneficial actions organizations can take are investing in more training and education at all levels, from non-technical employees and IT and cyber security teams to executive management.
4. *Not Providing the Right Training:* Survey respondents by far look to specific training courses (76 percent) and professional development organizations (71 percent) to build knowledge, skills and abilities (KSAs), rather than security certifications. Organizations can also employ more sophisticated and continuous training, such as “just-in-time” online training, and focus on specific skills including application and cloud security. And map these into training plans for overall career path development.
5. *Not Assuming a Perpetual Skills Shortage in Future Planning and Strategy*: Survey respondents say the number one cyber security challenge is the cyber security staff being understaffed for the size of their organization (29 percent). With no end in sight on this issue, organizations can create aggressive programs for recruiting talent from IT teams, especially IT operations and networking technology experience, as well as from business to bridge the cyber/business gap.

**To download the complete report**, available Monday November 13th, please visit: https://www.issa.org or http://www.esg-global.com/esg-issa-research-report.

**Methodology**

With over 343 information security professionals surveyed, representing organizations of all sizes and industry sectors and professionals located in all parts of the world, the research titled, “The Life and Times of Cyber Security Professionals” is the second annual cooperative research project by ESG and ISSA. It is the first global survey focused on the lifecycle of cyber security professional careers and their opinions about their organizations’ cyber security practices and well as the overall state of cyber security.

**About Enterprise Strategy Group**

The Enterprise Strategy Group (ESG) is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community. Recognized for its unique blend of capabilities—including market research, hands-on technical product testing, economic validation, and strategy consulting services—ESG is relied upon by IT professionals, technology vendors, investors, and the media to clarify the complex.

**About the ISSA**

The Information Systems Security Association (ISSA)TM 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. Visit ISSA on the web at www.issa.org and follow us on Twitter at @ISSAINTL.

###

**Media Contact:**
Leslie Kesselring
Kesselring Communications
503-358-1012
leslie@kesscomm.com