FOR EMBARGO 3:10PM ET

Cybersecurity Skills Shortage Worsening for Third Year In A Row, Sounding the Alarm for Business Leaders

Third annual global study from ESG and ISSA finds cybersecurity skills shortage impacts 74 percent of organizations; explores causes and consequences of cybersecurity job stress

Milford, MA and Vienna, VA – May 9, 2019 – The cybersecurity skills shortage is worsening for the third year in a row and has impacted nearly three quarters (74 percent) of organizations, as revealed today in the third annual global study of cybersecurity professionals by the Information Systems Security Association (ISSA) and independent industry analyst firm Enterprise Strategy Group (ESG).

Further the report confirms that the cybersecurity skills shortage continues to be the root cause of rising security incidents, as organizations remain plagued by a lack of end-user cybersecurity awareness and the inability to keep up with the growing cybersecurity workload. Almost half (48 percent) of respondents have experienced at least one security incident over the past two years with serious ramifications including lost productivity, significant resources for remediation, disruption of business processes and systems, and breaches of confidential data.

In fact, cybersecurity professionals are downright skeptical about their chances for success. Ninety-one (91) percent believe that most organizations are vulnerable to a significant cyber-attack. And an overwhelming 94 percent believe that the balance of power is with cyber-adversaries over cyber-defenders. With the battlefield advantage skewed, organizations face increasing and potentially devastating cyber-risks.

Despite these findings, for the third straight year, sixty-three (63) percent of organizations continue to fall behind in providing an adequate level of training for their cybersecurity professionals. The most acute skills shortages shifted this year to cloud security (33 percent), followed by application security (32 percent) and security analysis & investigations (30 percent).

In an era where business leaders are more reliant on technology for success and are facing more scrutiny and accountability than ever before, this lack of progress and the resulting cyber-risk for organizations and their shareholders, customers and business partners should be a cause for concern for business and technology leaders alike.

The research also indicates an alarming personal impact related to cybersecurity jobs. While cybersecurity professionals remain dedicated to their craft, attracted by the deep technical challenges and moral implications, this year's study explores for the first time the causes and consequences of stress and burnout, including:

- **Stressful aspects of the job**: Forty (40) percent responded with keeping up with security needs of new IT initiatives, followed closely by "shadow" IT initiatives, trying to get end-users to better understand cyber-risks and change their behavior, and trying to get the business to better understand cyber risks.
- **Added stress of new data privacy responsibilities**: Almost one year in, GDPR is in full swing, and cybersecurity teams may not be up to the task. Eighty-four (84) percent claim that the cybersecurity team at their organization has taken a more active role with

data privacy over the past 12 months, but 21 percent don't believe the cybersecurity team has been given clear directions and 23 percent don't believe the cybersecurity team has been given the right level of training.

- **Job-related pressures driving virtual CISO (vCISO) as attractive career option**: Ten (10) percent of organizations now employ a vCISO. Furthermore, 29 percent of CISOs are working as a vCISO while another 21 percent are considering it and 33 percent would consider it in the future. Almost half claim that working as a vCISO brings more variety and flexibility to a CISO position. CISOs are clearly seeking to avoid some of the politics and stress while taking more control of their careers.

"Based upon the results of this year's and past research projects, it is safe to conclude that cybersecurity progress has been marginal at best over the last three years. ESG and ISSA agree with security researcher, author and ISSA Hall of Fame recipient Bruce Schneier's quote, 'We may be making some cybersecurity improvements but we are getting worse faster.' This issue should be of concern to technologists, business executives and private citizens and continues to cause an existential threat to national security," said Jon Oltsik, Senior Principal Analyst and Fellow at the Enterprise Strategy Group (ESG) and the author of the report.

"Organizations are looking at the cybersecurity skills crisis in the wrong way: it is a business, not a technical, issue. Business executives need to acknowledge that they have a key role to play in addressing this problem by investing in their people. In an environment of a 'sellers market' with 77 percent of cybersecurity professionals solicited at least once per month, the research shows in order to retain and grow cybersecurity professionals at all levels, business leaders need to get involved by building a culture of support for security and value the function," said Candy Alexander, CISSP CISM, Executive Cybersecurity Consultant and ISSA International President..

Top 5 Roles in Addressing the Cybersecurity Skills Crisis

1. *Business Leaders*: Twenty-three (23) percent of respondents say business managers don't understand and/or support an appropriate level of cybersecurity. Job satisfaction and employee retention depends largely upon business leadership's commitment to cybersecurity, in addition to career incentives and competitive compensation. The number one recommended action is adding cybersecurity goals and metrics to IT and business managers.
2. *CISOs*: CISOs need to be more active with business executives. They want a seat at the board table. CISO success depends upon characteristics like communication skills, leadership skills, a strong relationship with business executives, and a strong relationship with the CIO and IT leadership team.
3. *Practitioners*: While 93 percent of survey respondents agree that cybersecurity professionals must keep up with their skills, 66 percent claim that cybersecurity job demands often preclude them from skills development. This imbalance must be addressed. Additionally, 57 percent of respondents say security certifications such as CISSP are far more useful in getting a job than doing a job. Prioritize practical skills development over certifications.
4. *HR and Recruiters*: Forty-one (41) percent of survey respondents say that their organization has had to recruit and train junior personnel rather than hire more experienced infosec professionals. Designing their own training program will develop future talent and loyalty. Casting a wider net beyond IT and finding transferable business skills and cross career transitions will help expand the pool of talent.

5. *Educators and Trainers*: KSA development with face-to-face interaction is most effective, such as attending specific cybersecurity training courses, participating in professional organizations and events, attending trade shows, and participating in on-the-job mentoring programs.

Finally, the private sector can only do so much. The public sector needs to help by investing more in training and education, public awareness, and scholarships and grants.

Download the report: https://www.issa.org/page/issa-esg-global-3rd-annual-cybersecurity-skills-survey or https://www.esg-global.com/esg-issa-research-report

Methodology
With a total survey sample of 267 cybersecurity professionals and ISSA members, representing organizations of all sizes and industry sectors and professionals located in all parts of the world, "The Life and Times of Cybersecurity Professionals, 2018: Third Annual Survey Results" is a cooperative research project by ESG and ISSA. This authoritative annual study is the only in-depth look at cybersecurity professional careers, lives and opinions about their organizations' cybersecurity practices and well as the overall state of cybersecurity.

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)™ is the community of choice for international cybersecurity 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, +1 503-358-1012, leslie@kesscomm.com