ESG and ISSA Research Reveals Cyber Security Profession at Risk

Findings from first global survey of cyber security professionals show 65% struggle to define their career path, while 46% are solicited for new jobs at least once per week, and outlines top 5 tips for taking control of the cyber security career lifecycle

Milford, MA and Reston, VA – October 5, 2016 – Amid the backdrop of National Cyber Security Awareness Month, the Information Systems Security Association (ISSA) and independent industry analyst firm Enterprise Strategy Group (ESG) revealed today the findings of the first global survey to capture the voice of cyber security professionals on the state of their profession. The alarming conclusion is that nearly two-thirds (65%) of cyber security professionals struggle to define their career paths.

This and other troubling trends uncovered in this research point to potentially unacceptable risks to individuals and their organizations alike. Two big "red flags": The majority of cyber security professionals aren't receiving the right level of skills development to address the rapidly evolving threat landscape. And the skills shortage has created a job market that represents an existential threat, adding job-related stress to cyber security personnel while making it harder for organizations to protect critical IT assets.

When it comes to the CISO, the research found that he or she succeeds or fails based upon leadership skills and face time with executive management and the board of directors. Also of concern is that cyber security relationships with business and IT groups need work.

The research comes at a time when there are more data breaches, net new malicious IP addresses created per day, zero-day vulnerabilities, credential thefts and phishing attempts than ever before. Many organizations are willingly bolstering their cyber security defenses and making cyber security a top business and IT priority, yet 46% of organizations claim to have a problematic shortage of cyber security skills according to previously published ESG research.

"This research paints an escalating and dangerous game of cyber security 'cat and mouse' and today's cyber security professionals reside on the front line of this perpetual battle, often knowing they are undermanned, underskilled and undersupported for the fight," said Jon Oltsik, Senior Principal Analyst, Enterprise Strategy Group (ESG).

Based upon the data collected, "The State of Cyber Security Professional Careers (Part I): An Annual Research Project (Part I)" conclusions include:

- **Nearly two-thirds (65%) of respondents do not have a clearly-defined career path or plan to take their careers to the next level:** This is likely due to the diversity of cyber security focus areas, the lack of a well-defined professional career development standard and map, and the rapid changes in the cyber security field itself.

- **Continuous cyber security training is lacking:** When asked if their current employer provides the cyber security team with the right level of training to keep up with business and IT risk, more than half (56%) of survey respondents answered "no," suggesting that their organizations needed to provide more or significantly more training for the cyber security staff.
- **Cyber security certifications are a mixed bag:** Over half (56%) of survey respondents had received a CISSP and felt it was a valuable certification for getting a job and gaining useful cyber security knowledge. Other than the CISSP certification however, cyber security professionals appear lukewarm on other types of industry certifications. Based upon this data, it appears that security certifications should be encouraged for specific roles and responsibilities, but downplayed as part of a cyber security professional's overall career and skills development.
- **Cyber security professionals are in extremely high demand.** Forty-six percent (46%) of cyber security professionals are solicited to consider other cyber security jobs (i.e. at other organizations) at least once per week. In other words, cyber security skills are a "sellers' market" where experienced professionals can easily find lucrative offers to leave one employer for another. This risk is especially high in lower paying industries like academia, health care, public sector, and retail.
- **Many CISOs are not getting enough face time in the boardroom, a significant contributing factor to CISO turnover.** While industry rhetoric claims that "cyber security is a boardroom issue," 44% of respondents believe that CISO participation with executive management is not at the right level today and should increase somewhat or significantly in the future. Alarmingly, this perspective is more common with more experienced cyber security managers (who should be working with the business) than cyber security staff members. When asked why CISOs tend to seek new jobs after a few short years, cyber security professionals responded that CISOs tend to move on when their organizations lack a serious cyber security culture (31%), when CISOs are not active participants with executives (30%), and when CISOs are offered higher compensation elsewhere (27%).
- **Internal relationships need work.** While many organizations consider the relationship between cyber security, business, and IT teams to be good, it is concerning that 20% of cyber security professionals say the relationship between cyber security and IT is fair or poor (surprising given that 78% of cyber security professionals got their start in IT) and 27% of survey respondents claim the relationship between cyber security and the business is fair or poor. The biggest cyber security/IT relationship issue selected relates to prioritizing tasks between the two groups while the biggest cyber security/business relationship challenge is aligning goals.

"These conclusions point to the need for business, IT, and cyber security managers, academics, and public policy leaders to take note of today's cyber security career morass and develop and promote more formal cyber security guidelines and frameworks that can guide cyber security professionals in their career development," said Candy Alexander, CISO, ISSA Cyber Security Career Lifecycle (CSCL) Chair. "Independent organizations such as the ISSA with its Cyber Security Career Lifecycle (CSCL) are taking the lead on such initiatives. This research data will help the ISSA strengthen its groundbreaking program."

The report also lays out the "Top 5 Research Implications for Cyber Security Professionals" as a guideline for taking control of the cyber security career lifecycle. Similarly, it lays out the "Top 5 Research Implications for Employers" to help businesses, non-profits, and government agencies appeal to cyber security professionals at large.

Added Oltsik, "In spite of these issues however, it is encouraging that 79% of survey respondents strongly agree or agree that they are happy as a cyber security professional. Together with a moral imperative that attracts people to the cyber security profession, this data point speaks volumes about cyber security professionals who are willing to passionately fight the good fight regardless of their personal situations."

To download the full report please visit: http://www.issa.org/esgsurvey/ or http://www.esg-global.com/ESG-ISSA-Research-Report.

To request the replay of today's press web conference discussing the study findings please contact: leslie@kesscomm.com.

Methodology

With over 437 information security professionals surveyed, representing organizations of all sizes and professionals located in all parts of the world, the research titled, "The State of Cyber Security Professional Careers (Part I): An Annual Research Project (Part I)" is a cooperative research project by ESG and ISSA and the first global survey focused on the lifecycle of cyber security professional careers. Part II in the series, to be published in November, will concentrate on cyber security professionals' opinions about their organizations' cyber security practices as 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)™ 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 represents 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 contacts:
Leslie Kesselring, Kesselring Communications
503-358-1012
leslie@kesscomm.com