FOR EMBARGO ONLY

Research Reveals “Human" Issues as Top Cyber Security and Business Risk

Second research report from ESG and ISSA’s groundbreaking global study of cyber security professionals sends strong message that critical infrastructure is vulnerable and they want more help from their national governments

Milford, MA and Reston, VA – December ~~xx~~12, 2016 – Building on the conclusions of the recent groundbreaking global study finding that the cybersecurity profession is at risk, the Information Systems Security Association (ISSA) and independent industry analyst firm Enterprise Strategy Group (ESG) revealed today new cyber security and business risks. In aggregate 54% cyber security professionals surveyed admitted that their organization experienced at least one type of security event over the past year and the clear majority (92%) believe that an average organization is vulnerable to some type of cyber-attack or data breach. Yet, surprisingly, none of the top contributors are related to cyber technology. Rather they point to human issues such as a lack of enough cyber security staff members as well as a lack of employee training and boardroom prioritization.

Further supporting this finding, 69% of cyber security professionals say the global cyber security skills shortage has had an impact on the organization they work for leading to excessive workloads, inappropriate skill levels, high turnover and an acute shortage especially in the areas of security analytics, application security and cloud security.

In this time with fluid world events, such as the U.S presidential transition, cyber security professionals surveyed also send a strong message to national government: The vast majority of believe that their nation’s critical infrastructure is extremely vulnerable or vulnerable to some type of significant cyber-attack and they want government more involved in cyber security strategies and defenses. Going further they recommend specific government actions that include providing better ways to share security information with the private sector, incentives to organizations that improve cyber security, and funding for cyber security training and education.

“There’s lots of research indicating a global cyber security skills shortage but there was almost nothing that looked at the associated ramifications. Based upon the two ESG/ISSA reports, we now know that beyond the personnel shortage alone, cyber security professionals aren’t receiving appropriate levels of training, face an increasing workload, and don’t always receive adequate support from the business,” said Jon Oltsik, Senior Principal Analyst at the Enterprise Strategy Group (ESG). “Simply stated, these findings represent an existential threat. How can we expect cyber security professionals to mitigate risk and stay ahead of cyber threats when they are understaffed, underskilled, and burned-out?”

Based upon the data collected from the first global survey to capture the voice of cyber security professionals on the state of their profession, this final report of the two-part series, titled "Through the Eyes of Cyber Security Professionals: Annual Research Report (Part II)," concludes:

- **People and organizations issues contribute to the onslaught of security incidents.** Nearly one-third (31%) of cyber security professionals say that the cyber security team is not large enough for the size of their organization, 26% point to a lack of training for non-technical employees, and 21% say that business and executive management tend to treat cyber security as a low priority. This data is especially troubling as it suggests that many organizations continue to lack a proportional commitment to cyber security.
- **Most organizations are feeling the effect of the global cyber security skills shortage.** Sixty-nine percent of cyber security professionals say that the global cyber security skills shortage has had an impact on the organization they work for. What type of impact? More than half (54%) say the cyber security skills shortage has resulted in an increasing workload on existing staff, 35% say it has forced them to hire and train junior employees rather than bring on more experienced cyber security professionals, and 35% say that the cyber security skills shortage has led to the inability to learn or fully utilize some of their security technologies.
- **Cyber security professionals have several suggestions to help improve the current situation.** Cyber security professionals were asked what type of cyber security actions would be most beneficial to help their organizations. Forty-one percent suggested increasing the cyber security budget, 40% proposed adding cyber security goals and metrics to business and IT managers' objectives, 39% recommended increasing cyber security training for non-technical employees, and 39% advised hiring more cyber security professionals.
- **Critical infrastructure is very vulnerable to cyber-attacks.** A majority (62%) of cyber security professionals believe that their country's critical infrastructure services like electric power, telecommunications, and water are very vulnerable to some type of significant cyber-attack.
- **Government cyber security tends to be incoherent and incomplete.** More than one-fourth (26%) of cyber security professionals surveyed say that their country's cyber security strategy is extremely unclear and not at all thorough while another 37% claim that their country's cyber security strategy is somewhat unclear and not very thorough. This leads to an obvious conclusion: If cyber security professionals don't understand their country's cyber security strategy, who does?
- **Cyber security professionals want more help from their governments.** More than half (57%) of cyber security professionals believe that their government should be significantly more active with cyber security strategy and defense while another 32% say that their government should be somewhat more active with cyber security strategy and defense.

"The results gleaned from this research are both alarming and enlightening. Alarming in the sense that if we don't collectively pay attention to the cries for help, we will put businesses unnecessarily at risk. Enlightening in that organizations need to be willing to invest in their cyber

security professionals, with clearly defined career paths and skills development in order to hire and retain qualified employees," said Candy Alexander, Cyber Security Consultant and ISSA's Chair of the Cyber Security Career Lifecycle. "This research data will help the ISSA and other professional groups to clearly define career paths for our profession."

The report also lays out the "Top 5 Research Implications" as a guideline for cyber security professionals and the organizations they work for. Added Oltsik, "Assume your organization will experience one or several cyber-attacks or data breaches and take the cyber security skills shortage into account as part of every initiative and decision. Push for more all-inclusive cyber security training and, as importantly, get involved in educating and lobbying business executives and lobby government legislators alike."

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

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

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