The Impact of the COVID-19 Pandemic on Cybersecurity

Assessment of challenges posed by the pandemic ranging from spike in cyberattacks to lackluster support for cybersecurity prioritization

Milford, MA and Vienna, VA, July 30, 2020 (BUSINESSWIRE) – The COVID-19 pandemic has presented a once-in-a-lifetime opportunity for hackers and online scammers, and cybersecurity professionals saw a 63 percent increase in cyber-attacks related to the pandemic, according to a survey released by the Information Systems Security Association (ISSA) and independent industry analyst firm Enterprise Strategy Group (ESG). As the global impact of COVID-19 manifested itself in the middle of March, ESG and ISSA conducted an in-depth survey in April 2020 as a point in time assessment of challenges posed by the pandemic.

Based on the data gathered for this project, the report highlights the following:

- **Organizations were only fairly prepared for the global pandemic.** Thirty-nine percent of respondents claim that they were very prepared to secure WFH devices and applications while 34 percent were prepared. Twenty-seven percent were underprepared. Therefore, the pandemic drove rapid changes, changing workloads, and new priorities.

- **COVID-19 and WFH are driving improved collaboration.** Slightly more than one-third of organizations have experienced significant improvement in coordination between business, IT, and security executives as a result of COVID-19 issues and 38 percent have seen marginal relationship improvements.

- **COVID-19/WFH have had an impact on cybersecurity professionals and their organizations alike**. The research indicates that COVID-19 has forced cybersecurity professionals to change their priorities/activities, increased their workloads, increased the number of meetings they have had to attend, and increased the stress levels associated with their jobs. Meanwhile 48 percent say that WFH has impacted the security team's ability to support new business applications/initiatives.

- **Most organizations don't believe the pandemic will increase 2020 cybersecurity spending.** Only 20 percent believe that COVID-19 security requirements will lead to an increase in security spending in 2020, while 25 percent think their organizations will be forced to decrease security spending this year. Where they expect their spending to increase, at least half pointed to priority areas being identity and access management, endpoint security, web and email security, and data security.

- **COVID-19 may impact cybersecurity priorities.** ESG/ISSA believes that while it is noteworthy that 30% of the cybersecurity professionals participating in this project say that cybersecurity will be a higher priority, 70% report that they don’t know or don’t believe that this crisis will lead to cybersecurity becoming a higher priority.

Finally, is COVID-19 causing cybersecurity professionals to be concerned about their jobs or career choice? Overall, the answer seems to be “no” to both questions, however, the data seems to indicate that there is more uncertainty in the short-term about current cybersecurity jobs.

“COVID-19 had a wide-ranging impact on individuals on the security staff. With 84 percent of cybersecurity professionals working exclusively from home during the pandemic and almost two-thirds believing that their organizations will be more flexible with work-at-home policies moving forward, COVID-19 has personally impacted cybersecurity professionals in their jobs and in their lives. This is in addition to the ongoing impact on organizations and security teams from the yearly worsening problem of the cybersecurity skills shortage,” Jon Oltsik, Senior Principal Analyst and ESG Fellow.

“While it’s promising to see that the majority of organizations were able to handle the COVID-19 pandemic fairly well, it is surprising that we are not seeing an increase in cybersecurity spending or prioritization following this event. If anything this should serve as a wakeup call that cybersecurity is what enables businesses to remain open and operational. Organizations prioritizing cybersecurity as a result of the pandemic will likely emerge as leaders in the next wave of cybersecurity process innovation and best practices,” said Candy Alexander, Board President, ISSA International.

The full report, “The Impact of the COVID-19 Pandemic on Cybersecurity,” represents 364 cybersecurity and IT professionals from the global ISSA member list and contains further research on the effects COVID-19 had on the cybersecurity profession. 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.