# ISACA Survey: Cybersecurity Attacks Are Rising During COVID-19, But Only Half of Organisations Say Their Security Teams Are Prepared for Them

Sydney, Australia (4 May 2020) – Only 51 per cent of technology professionals and leaders are highly confident that their cybersecurity teams are ready to detect and respond to the rising cybersecurity attacks during COVID-19, according to new research by global association ISACA. Additionally, only 59 per cent say their cybersecurity team has the necessary tools and resources at home to perform their job effectively.

This presents a problem, as 58 per cent of respondents say threat actors are taking advantage of the pandemic to disrupt organisations, and 92 per cent say cyberattacks on individuals are increasing. Cybersecurity professionals have seen a spike in COVID-19 phishing schemes promising government stimulus handouts, and even a financial relief package from the World Health Organization.

While 80 per cent of organisations shared cyber risk best practices for working at home as self-isolation measures began, 87 per cent of respondents still say the rapid transition to remote work has increased data protection and privacy risk.

“Organisations are rapidly and aggressively moving toward new ways of doing business during this time, which is a very positive thing, but it can also lead to making compromises that can leave them vulnerable to threats,” says ISACA CEO David Samuelson. “A surge in the number of remote workers means there is a greater attack surface. Remote work is critically important right now, so security has to be at the forefront along with employee education. ISACA professionals have an especially critical role to play in protecting their enterprises, customers and stakeholders during this pandemic.”

Upskilling & Reskilling during COVID-19

ISACA is also seeing an uptake in professionals utilising this time to increase learnings and focus on career development to pivot into cybersecurity roles. In response to COVID-19, ISACA has expanded its online certification offerings, including exam-taking from home via remote proctoring, to ensure learning and certification opportunities are maximised during this time.

According to the State of Cybersecurity 2020 report, prior to COVID-19, 62 per cent of respondents believe their organisation’s cybersecurity teams are understaffed and many organisations struggle to find the right candidates with the right skills and experience to meet the demands of those roles. Job opportunities in cybersecurity are predicted to increase, as people continue to embrace new technologies and evolve remote working options, which can leave organisations more vulnerable to cyberattacks. Hence, making certifications available online assists professionals to upskill and reskill during this time.

Outlook for Employment Post-COVID-19

Looking toward the economic and personal effects, the COVID-19 research shows most of the professionals surveyed believe their jobs are safe. Ten per cent think a job loss is likely and 1 per cent has been asked to take leave without pay. However, while their own positions are stable, respondents are still extremely concerned about these wider impacts of the novel coronavirus:

Economic impact on my national economy (49 per cent)Health of family and friends (44 per cent)Personal health (30 per cent)Economic impact on my organisation (24 per cent)

COVID-19 Impact on Business Operations

While respondents report being highly satisfied with their organisation’s internal communications, business continuity plans and executive leadership related to COVID-19, their organisations have not been able to avoid the negative effects, including:

Decreased revenues/sales (46 per cent)Reduced overall productivity (37 per cent—more executives than practitioners think this is the case)Reduced budgets (32 per cent)Supply chain problems (22 per cent)Closed business operations (19 per cent)The majority of respondents expect normal business operations to resume by Q3 2020.

“It’s hard to predict what ‘normal’ will look like in the short term,” said ISACA CTO Simona Rollinson. “What we do know is that tech professionals, including the IT audit, risk, governance and security professionals in our community, are more necessary than ever to their enterprises, and they are well-positioned to adapt and even thrive, regardless of what changes may be in store.”

ISACA surveyed more than 3,700 IT audit, risk, governance and cybersecurity professionals from 123 countries in mid-April to assess the impact of

COVID-19 on their organisations and their own jobs.

For more information on ISACA's COVID-19 study, visit www.isaca.org/covid19study. ISACA's COVID-19 resource centre, which contains resources on business continuity, secure remote work and virtual learning, is available here. More details about ISACA's globally recognised certifications, with exams that can be conducted at home with live remote proctoring, is provided here.

About ISACA
For more than 50 years, ISACA® (www.isaca.org) has advanced the best talent, expertise and learning in technology. ISACA equips individuals with knowledge, credentials, education and community to progress their careers and transform their organisations and enables enterprises to train and build quality teams. ISACA is a global professional association and learning organisation with 145,000 members who work in information security, governance, assurance, risk and privacy. It has a presence in 188 countries, including more than 220 chapters worldwide.

Twitter: www.twitter.com/ISACANews
LinkedIn: www.linkedin.com/company/isaca
Facebook: www.facebook.com/ISACAGlobal
Instagram: www.instagram.com/isacanews

Contact:
Julie Fenwick, jfenwick@daylightagency.com.au +1 61 468 901 655
Karen Keech, kkeech@daylightagency.com.au, + 61 411 052 408

**Contacts**

Julie Fenwick
The Daylight Agency
mailto:
Karen Keech
0411 052 408
mailto: