IAITAM: TIKTOK "UNNECESSARILY ENDANGERS DATA" ON PHONES USED BY EMPLOYEES WORKING FROM HOME DURING COVID-19

Popular App Revives Earlier Concerns About Fitbit, Pokémon Go Licenses and App Permissions That Could Jeopardize Company/Client Data

CANTON, OHIO – July 15, 2020 – The nation of India, the U.S. military, and banking giant Wells Fargo already have either banned TikTok app use altogether or at least on company mobile devices. Should your organization follow suit and prohibit the popular app TikTok on company and even personal phones? Today, the International Association of IT Asset Managers (IAITAM) warned that allowing employees to use TikTok on any devices (including personal cell phones and tablets in a work-from-home context) with direct access to corporate data is "not consistent with maintaining data integrity."

The TikTok app is taking the world by storm, with controversy brewing over whether the app's open-ended permissions pose security risks for corporations, government agencies and other organizations particularly during a time when many employees are still working from home (WFH) due to COVID-19.

Concerns about the Chinese-owned TikTok are reminiscent of earlier security worries about Fitbit and Pokémon Go. In 2016, IAITAM called on corporations to ban the installation and use of Pokémon Go on both corporate-owned, business-only (COBO) phones/tablets and "bring your own device" (BYOD) phones/tablets with direct access to sensitive corporate information and accounts. In 2019, IAITAM advocated against Microsoft's policy decision to let end-users buy some of their own apps and licenses through Office 365, bringing up concerns over how businesses would track IT assets to ensure compliance. Due to such criticism, the technology giant reversed its decision.

The TikTok app has been found gathering data that includes the user's clipboard history, location and GPS data, much like the Fitbit security breaches that the Department of Defense experienced in 2018, where fitness trackers used location data to map military bases while soldiers exercised.

Dr. Barbara Rembiesa, president and CEO of IAITAM, said: **"The TikTok app unnecessarily endangers data in a way that any government agency or corporation should be concerned about. Combine that with the blending of corporate and personal assets due to work-from-home conditions for employees and you have a perfect storm for sensitive data to be placed into the wrong hands. As things stand today, allowing TikTok in or near your organization's environment is not consistent with maintaining data integrity."**

Rembiesa continued: **"Acceptable data risk needs to be ascertained prior to downloading software and such software should be managed by an IT asset manager. The risk posed by the data permissions of TikTok does not meet data security best practices. Diligence and**

education on ITAM procedures are essential for businesses to implement smart digital policies and mitigate security risks."

Since March, IAITAM has been at the forefront of work-from-home data concerns during the COVID-19 pandemic, issuing multiple warnings on "nightmare data risks", tech headaches and challenges associated with transitioning to work from home.

Following ITAM best practices is a roadmap for organizations to protect and get the most out of their IT assets. IAITAM offers courses and training opportunities throughout the year for agencies and businesses seeking to strengthen their cybersecurity and IT asset management.

ABOUT IAITAM

The International Association of Information Technology Asset Managers, Inc., is the professional association for individuals and organizations involved in any aspect of IT Asset Management, Software Asset Management (SAM), Hardware Asset Management, Mobile Asset Management, IT Asset Disposition and the lifecycle processes supporting IT Asset Management in organizations and industry across the globe. IAITAM certifications are the only IT Asset Management certifications that are recognized worldwide. For more information, visit www.iaitam.org.

MEDIA CONTACT: Whitney Dunlap, (703) 229-1489 or wdunlap@hastingsgroup.com