IAITAM: GOOGLE DRIVE POSES SPECIAL CHALLENGES BUSINESSES RARELY CONSIDER IN ADVANCE

Reliance on Single Password for Google Combined With Heavy Exposure From "Bring Your Own Device" Smartphones and Tablets Poses Special Risks for Unwary Employers.

CANTON, OH – July 12, 2018 – Google Drive is free, relatively easy to use, and available to everyone with a Gmail account. No wonder that the cloud-based server storage service (in the same league as Dropbox, Microsoft OneDrive, and others) is seen as such a comfortable fit for hundreds of thousands of medium- and small-sized businesses that need a place to put documents and to work on them remotely. But Google Drive can be a "nightmare" for unwary businesses that fail to understand the associated risks and how to manage them.

As Dr. Barbara Rembiesa, president and CEO of the International Association of IT Asset Managers (IAITAM) points out, the time to look at Google Drive security issues is on the front end of the process. But few businesses do so; 50 percent of those surveyed recently were so confident in the security of their cloud services that they never even bothered to explore the issue. Burying your head in the sand is never a solution, given that 15 percent of business cloud users already have been hacked. If a catastrophic loss of confidential business information is what it takes to prompt you to look into Google Drive security, it's already too late.

IAITAM President and CEO Barbara Rembiesa said: **"Google Drive is just like any other cloud services. You have to check it out. You have to make sure it's the right fit. You have to have all your Information Technology Asset Management (ITAM) rules and procedures in place and you have to be vigilant as a hawk on an ongoing basis. There are so many things that can go wrong and so many loose ends, that many organizations will find that it's a bit of a nightmare. However, proceeding in blissful ignorance is an even worse option."**

Here's how Google Drive works: The files you add to your Google Drive app or folder are stored on servers in secure data centers. Your data stored with Google is encrypted during transfer from your computer — and on Google Drive servers. Google also tells users that unless they publish a file, search engines won't be able to find the files and open them. Google doesn't allow search engine crawlers -- the applications that crawl through the Internet looking for keywords – access to the content of Google Docs.

But there are some real vulnerabilities to Google Drive that need to be considered very carefully by business owners:

- ***One password is your passport to the world of Google.*** That makes it easy to get into Gmail and Google Drive … and, in fact, maybe it makes it too easy. An employee who stays logged in to Gmail on their desktop or smartphone is also logged into Google Drive. Consider these facts: 70 million smartphones are lost each year, with only 7 percent recovered; 4.3 percent of company-issued smartphones are lost or stolen every year; 52 percent of devices are stolen from the office/workplace, and 24 percent while at conferences. That means millions of phones and laptops are stolen every year where people are signed into Google and, therefore, Google Drive. Unfortunately, Google Drive does not automatically log users out after a period of inactivity.

- ***Even if your company uses good password "hygiene" when it comes to company accounts, you may be laxer when it comes to personal Gmail accounts used to access Google Drive.*** This is a problem particularly for medium- and small-sized companies that may be using the free or low-cost version of Google Drive. Your Google Drive is every bit as vulnerable as every employee who accesses it with a Google password that is weak, predictable and easily cracked. There are many wrinkles to this: How tough are your standards for part-time/seasonal employees and independent contractors who access your Drive? What about clients who are given permissions to review and edit documents and spreadsheets under production?

- ***Google is catnip for hackers.*** It seems like some software provider, app maker or website builder is always the top target for hackers. For years now, Google is a prime target for hackers. In one recent case, 24 million Gmail accounts were exposed. And there have been several "phishing" attacks over the years to trick Google users to give up their credentials. While you may consider your company too small or unremarkable to be a target of hacking, that does not mean you cannot get caught up in a wider hack of Google that leaves all the confidential business information in your files vulnerable.

- ***Confusing Google Drive "permission" settings can lead to disaster.*** Some users may find the Google Drive "permission" settings too confusing. And it's the "permission" part of Google Drive that companies using Google Docs should be very cautious about. Understand how your employees are using and sharing data is critical. Are they limiting it to their own view or only certain people? Or, are they opening it up to everyone on your company's domain … or the whole Internet? It's easy to get this wrong and the consequences for confidential information can be huge.

These are just some of the challenges of dealing with a cloud server for your business. When it comes to Google Drive, one concern is "offboarding." If an employee invited to use the Drive is fired but retains their personal Google account used to access the drive, how effective will your organization be in scrubbing them from what may well be a dozen or more permissions to access certain folders and files?

IAITAM's Rembiesa added: **"We cannot rely on vendor solutions to substitute for internal security processes. That is something we must take accountability for as an organization and as a profession. The foundational step is knowing what devices are logged in, where those devices are, and who they belong to. That is what IT Asset Management does. 'You can't secure what you don't know' has been a rallying call of mine for years. As popularity of cloud-based solutions such as Google Drive continue to trend upward, the problem will continue to grow and expand. We must be proactive and develop internal processes that focus on data management and security instead of waiting for vendors to provide that as a feature within their products."**

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, or the IAITAM mobile app on Google Play or the iTunes App Store.

MEDIA CONTACT: Alex Frank, (703) 276-3264 or afrank@hastingsgroup.com.