IAITAM: TOO MANY COMPANIES, AGENCIES WITH VULNERABILITIES "WIDE OPEN TO ATTACK" FROM BREACHES DURING COVID-19 STAY-AT-HOME SHUTDOWNS

After Issuing Repeated Warnings, IAITAM Highlights 4 Biggest Problems Happening Now.

CANTON, OH – April 20, 2020 – Today, the International Association of IT Asset Managers (IAITAM) is warning that breaches of corporate and government data appear to be running at a level even higher than experts had feared going into stay-at-home orders due to COVID-19.

Last month, IAITAM repeatedly warned of "nightmare data risks" for unprepared government agencies & companies, especially as end-of-the month billing procedures were being carried out remotely.

IAITAM President and CEO Dr. Barbara Rembiesa said: **"We anticipated that things would get bad. Companies and agencies may be hoping and praying they are safe, but the work-from-home environment has created a multitude of opportunities for leaks. Too many organizations have left themselves wide open for attack. Understanding the pathways for access within a company's data network is a valuable lens for businesses and agencies to avert leaking their own assets."**

Based on its preliminary analysis of early published reports, IAITAM is breaking down the biggest problems into four categories:

1. **Assets left unsecure** → An intentional decision to make devices less secure to allow for work from home (WFH) use. One example would involve removing admin permissions so that employees can complete the task without administrator oversight. Another would be allowing the use of "unpatched" business computers that allow hackers to load malicious files with admin privileges. In some cases, companies with high-end virtual private networks (VPNs) pre-loaded on business computers are allowing people to work from home on personal devices either with no VPN or with a lower-end virtual private network that may be less hacker resistant.

2. **"New" assets created** → More and more reports are emerging of companies purchasing new devices or technology to account for employees working from home. In one case reported directly to IAITAM a national health care company ordered 9,000 new laptop computers from a major online company and gave its IT department less than a week to prep the new machines and deliver them to users, who had little or no time for training and other security-related instructions. The concern: The more corporate assets that you have, the higher risk of intrusion. Each asset becomes a doorway or entry point for a breach, particularly when it (or its user) are underprepared. IT Asset Managers help with this by providing the data necessary for corporate security teams to know what exists, where it exists, and what is on the device.

3. **Assets now unsecure in at-home environments** → Many company devices were deployed into a WFH situation quickly, leaving little time to ensure that they would be secure via a virtual private network (VPN) or other means. Just last week, school districts in Oakland and Berkeley, California unwittingly became an accomplice in their own data breach by accidentally making Google Classroom documents public, which contained access codes and passwords for Zoom meetings, as well as student's names and comments.

4. **Employees unwittingly inviting in the intrusion** → Human error allows for mistakes and creates a vulnerability (i.e. clicking on phishing emails or downloading malware). Google reported last week that it is stopping 18 million coronavirus scam-related emails every day, many of them targeting cash strapped businesses looking for loans or other capital. An internal memo from NASA on April 6th revealed that increased cybersecurity attacks had been directed at their employees working remotely. These phishing attempts were disguised as appeals for help, disinformation campaigns or new information about COVID-19, to gain login credentials or install malicious software. This is a prime example of how an employee could unwittingly invite in an intrusion. IT Asset Managers are at the forefront of education and communication campaigns within organizations to help teach end users what they should and should not be doing.

Even companies that do not make a mistake themselves could still find themselves the victim of a coronavirus-related breach. Earlier this month, The Small Business Administration experienced a glitch with a coronavirus loan relief fund platform that publicly leaked the personally identifiable information of business owners across the nation.

The good news is that most or all of these issues can be mitigated with proper IT asset management (ITAM). Professionals in the ITAM industry facilitate corporate asset protection. Uncovering the vulnerabilities now, and then putting an action plan into place will save companies money in the end. If companies and businesses act now, they can turn today's crisis into tomorrow's opportunity.

IAITAM President and CEO Dr. Barbara Rembiesa recently went on camera to share more about what companies and government agencies should be doing.

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.