IAITAM: SUPERMICRO MICROCHIP HACK COULD HAVE BEEN PREVENTED IF MORE COMPANIES FOLLOWED RULES LIKE APPLE

Scandal Involving Major Companies, Pentagon, Congress, Homeland Security Illustrates Need for Proper ITAM Procedures; No Firm or Agency Gets a Pass Just Because the Global Supply Chain is Complex.

CANTON, OH – October 11, 2018 – Could the insertion of grain-of-rice-sized microchips in servers headed for Amazon, Apple, other leading companies, the Department of Defense, Congress, and Homeland Security been detected and exposed earlier? Not only could this have happened, but it should have as a result of adhering to good Information Technology Asset Management (ITAM) procedures, according to the International Association of IT Asset Managers (IAITAM).

IAITAM noted that Apple appears to have applied at least some proper ITAM practices for equipment acquisition and detected problems with the Super Micro Computer Inc. (Supermicro) servers. The fact that Apple spotted issues in 2015 and stopped using Supermicro shows that ITAM Vendor Management best practices work.

IAITAM President and CEO Barbara Rembiesa said: **"The global supply chain is complex, but companies do not get a pass because of that when it comes to managing the IT assets that they use or sell to others. Companies need to follow proper Information Technology Asset Management practices to make sure that every piece of equipment is needed, configured and functioning as intended, and is monitored on a continuing basis after use starts. The Supermicro scandal shows that even the biggest companies and government agencies don't do their homework when it comes to the handling of new IT equipment."**

Bloomberg was the first to report that unauthorized microchips have been inserted into motherboards bound for servers sold by California-based company Supermicro. According to the news account, the secret microchips are capable of altering server code, downloading software to get through passwords and other encryptions. No technology for consumers to detect the microchips has been invented. The microchips, which have been linked to Chinese interests, are meant to steal corporate secrets and breach government networks.

Rembiesa highlighted three notable moments on the Supermicro timeline:

1) **Microchips Installed:** Bloomberg reported that thieves visited the factories and threatened and bribed their way into getting the new microchips installed in the motherboards. It is unclear precisely when this hardware hack, commonly known as "seeding," started. However, it was reported that Amazon was made aware of issues with Supermicro as a vendor in 2015 when the company hired a third-party to investigate the servers. The malicious chips were discovered and reported to the FBI.

2) **Apple Reacts:** Meanwhile, Apple began disposing of Supermicro servers around that time for an unrevealed reason. The company has disputed the Bloomberg account, but it does appear to have been alone in using ITAM measures to detect, isolate and end the problem in its own operation.

3) **The Pentagon's Summit:** In September of 2015 the Pentagon organized and invited top technologists to a meeting in McLean, Virginia. Attendees were briefed on newly discovered

hardware hacks. Supermicro's name was not mentioned. However, it is assumed that the microchips on their servers were the reason why the summit was held.

Rembiesa noted: **"Fortunately, there are breadcrumbs on this trail and they can be followed. Assuming proper documentation procedures have been followed, authorities should be able to use invoices, shipping manifests, and other documents to help with their missions. Proper documentation is a best practice of a well-run ITAM program."**

How could ITAM help prevent a Supermicro-like situation in the future?

ITAM involves a detailed process that focuses on optimal acquisitions of hardware, software, and any other IT asset an organization buys or leases. Stages of this acquisition process include justifying the purchase, managing negotiations with vendors and assembling vital documents, such as the terms and conditions, among others.

A key part of the process is the testing of the hardware or software. This stage determines whether the asset is appropriate and compatible. At some point during their relationship with Supermicro, Apple determined that the servers were inappropriate and incompatible. Apple's ITAM staff identified Supermicro as a threat during the "testing" section of the process. They stopped buying from Supermicro and also returned the products already purchased.

Beyond the acquisition process, Rembiesa said that IT Asset Managers should be immediately consulted in a situation like this because of their use of discovery data within an organization's IT Asset Repository. This process helps IT Asset Managers identify exactly where hardware is located with an organization, cutting down immensely on the time needed to find flawed or sabotaged pieces of equipment. The quicker the hardware is identified and then "unplugged" from an organization's environment, the less damage the sabotaged item or items can do.

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.