# IAITAM: UNPREPARED COMPANIES, GOV'T AGENCIES SENDING WORKERS HOME IN RESPONSE TO CORONAVIRUS FACE "NIGHTMARE" DATA RISKS

***Even Companies That Send Employees Home With Proper Safeguards Face Challenges, but Those Relying on Uncontrolled Employee-Owned Phones & Computers to Get Work Done "Are Sitting Ducks".***

**CANTON, OH – March 17, 2020 –** Many companies and government agencies have already sent employees home to work remotely in response to concerns about the coronavirus. This week, thousands of additional employers will likely follow suit until concerns about the contagion ease. The International Association of IT Asset Managers (IAITAM) is warning that most employers may have rushed into making their decision without thinking through how to secure their most sensitive data.

Dr. Barbara Rembiesa, president and CEO of IAITAM, said: **"We always say that you can't manage what you don't know about and that is going to be a truth with nightmare consequences for many companies and government agencies struggling to respond to the coronavirus situation. The impulse to send employees home to work is understandable, but companies and agencies without business continuity (BC) plans with a strong IT Asset Management (ITAM) component are going to be sitting ducks for breaches, hacking and data that is out there in the wild beyond the control of the company."**

As an example, Rembiesa cited a 2015 IAITAM report that found 17 percent of U.S. Securities and Exchange Commission (SEC) laptops were not where they were supposed to be and 22 percent had incorrect user information. The Washington, D.C. office of the SEC sent all employees home to work last week due to the discovery of a coronavirus case in the agency's headquarters. Under the circumstances cited in the IAITAM report, the SEC would have little confidence that it knows who is working remotely on which machines and under what circumstances.

In the best-case scenario right now, a company or agency has a Business Continuity plan that incorporates ITAM and one that can send employees home with IT assets that are accounted for and working properly. Under this approach some employees using high-end, expensive computers and other equipment may not be able to work from home, while others requiring only a laptop and word-processing software will be able to operate offsite with ease.

If your company is sending home people with equipment, IAITAM has this advice:

1. ***Sign out and track all IT assets that are being taken home.*** No IT assets should be allowed to leave a company site for the first time without formally accounting for each movement.

2. ***Make sure solid firewall and passcode protections are in place for accessing company systems.*** Companies and agencies that plan properly will "scale up" to accommodate a shift in traffic from the workplace to remote access.

3. ***Consider requiring employees to sign a Non-Disclosure Agreement (NDA) about the data they will have access to outside the office.*** The data is often significantly more valuable than the IT assets in which it is contained. Vital company information may be at stake and an NDA sends a message to employees that they have serious responsibilities that must be honored and respected.

4. ***Provide education and training to employees about how to responsibly manage their equipment and the company's data.*** For example, parents who are accustomed to allowing a child or spouse to use a personal smartphone or computer must be coached to avoid doing so with company IT assets. Companies may also elect to forbid the use of company IT assets on public Wi-Fi networks, such as coffee shops and fast-food restaurants.

5. ***Monitor employee data use and other remote practices.*** It would be nice to assume everyone will follow the rules and be a team player, but that doesn't always happen. Any potential for mischief or data abuse may be heightened in a work-from-home environment. Remember that most data breaches are caused by insiders, not outside hackers.

6. ***Tighten up the reins on Bring Your Own Device (BYOD) practices.*** The reality is that the longer someone is out of the office, the more likely it is that they will do company business on their personal smartphone, computer, tablet or other Bring Your Own Device (BYOD) asset. A device that is BYOD could simply be a personal phone that receives work emails. If the employee's contract or policy language does not give the data rights to the organization, the IT Asset Manager will need to make an addendum giving the rights to the organization. The employee may own the device, but the work-related data is 100 percent owned by the company.

What about companies and government agencies that did not invoke their BC plans with ITAM protections built in, and are now sending employees home to work things out as best one can on their own personal devices? (This could also apply to companies and agencies that have such plans in place, and ITAM, but rushed ahead out of coronavirus fears and did not call on the protective provisions.) For those companies and agencies, the list of potential problems is long:

1. ***Companies and agencies will have little or no information about the devices being used to conduct company business.*** In the absence of the most basic mobile device management (MDM) system, companies will be almost completely blind as to who is accessing their data.

2. ***Companies and agencies that do not require their workers to operate remotely through a virtual private network (VPN) will be relying on personal Wi-Fi systems that may be entirely insecure and/or already corrupted.*** Unprepared companies may also find that their VPNs are unprepared for a tidal wave of outside access. Companies that allow employees to use BYOD devices to do business on public Wi-Fi systems may be even more vulnerable to attack.

3. ***The longer employees are working remotely in a vulnerable state, the bigger a target they may become for phishing and other attacks.*** Already, there have been countless coronavirus-related attacks. Those working at major companies and government agencies may find themselves in the crosshairs of such sophisticated schemes. In the absence of training and ongoing guidance from their company, the sensitive data on personal devices could be at considerable risk.

4. ***Data on personal devices (outside the reach of a company or government agency) likely will remain there when the employee returns to work.*** This creates a huge risk if the personal device is "handed down," sold to a third-party or improperly disposed of. In these scenarios, the exposure of sensitive company data may be entirely unintentional and end up becoming public.

**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.