EINPRESSWIRE

Is Working From Home an Unknown Security Risk? What is the price of this convenience? Axios Investigations Firm Reports

More people are working from home due to the increased risk of COVID. However, does this convenience allow for a potential security threat unforeseen?

Informational Security

WASHINGTON, DC, UNITED STATES, December 16, 2020 / EINPresswire.com/ -- More companies and government agencies are allowing people to work from home due to a potential increased risk of COVID 19 infection spreading within the workplace. However, does this convenience allow for a potential security threat unforeseen? With billions spent on biometric login security, two-way authentications, CAC card or chip readers, and VPN's to protect the online user from an online security threat. Unfortunately, now what was once a protected workplace environment to speak about sensitive discussions is no longer secure as we discuss work from our homes, apartments, or hotels.

> We don't need to walk in a minefield and hope that one day we don't trip the wire.”
>
> *CEO, Axios Investigations Firm, LLC*

In 2019, 1 in 5 corporations have had their intellectual property stolen from a foreign government according to an article from CNBC. According to the IP Commission, a commission on the Theft of American Intellectual Property, states that the effect on our U.S economy is estimated to be nearly "$600 billion annually." This is a significant impact on companies. With more people working from home this type of workplace change could allow for both foreign governments or competing companies to try and find additional opportunities to breach through operational security (OPSEC) procedures. Most OPSEC procedures were created when the employee was working within the safety and security of the brick and mortar workplace and now they may need to be reassessed.

Axios Investigations Firm has received an increased amount of calls on this subject and has worked to address the issue in a recent video discussing the importance of TSCM (Technical

Surveillance Counter-Measures) or more simply described as "Bug Sweeping." Bug Sweeping is a term that describes where the technician uses electronic counter-surveillance equipment to conduct a radio frequency (RF) scan of the desired area. This can be done remotely and in a corporate or home environment. As technology continues to improve over time the hidden devices are becoming smaller and can be hidden with ease and almost without detection. That is why these types of sweeps need to be done by a highly trained and licensed professional.

Speaking to a contractor with the National Security Agency under the condition of anonymity stating, "this could be a potentially bad situation. Most government employees that have sensitive to secret conversations are required to use a SCIF (Sensitive Compartmented Information Facility.) Unfortunately, people at home do not have the ability to do so." The contractor encourages companies and government agencies to re-evaluate their protocols on how employees conduct business meetings at home and if it makes sense to conduct an electronic security sweep prior to a meeting it would be encouraged to do so.

Axios Investigations Firm Logo

Service Disabled Veteran Owned Business

Axios Investigations Firm CEO Jereme D also agrees with this sentiment stating, "although this has not become a national issue as of yet. We need to be more diligent and proactive when it comes to our security within the workplace. We don't need to walk in a minefield and hope that one day we don't trip the wire." Operational security measures is a living and moving thing and must change with the times. It cannot be stagnant. He is working to get the message out and have his company to be at the forefront of this potentially disastrous issue.

Denise Carter
Axios Investigations Firm, LLC
+1 833-462-9467
clientservices@axiosinvestigations.com
Visit us on social media:
Facebook
Twitter
LinkedIn