REVEALRISK
SECURE YOUR BUSINESS

BACK TO “THE OFFICE” - WHEREVER THAT IS!

Plans for the “office return” vary drastically. Some companies have decided to be fully remote with smaller corporate offices for centralized meetings. Some companies never left the office. Manufacturing companies, companies with laboratories, and other physical hands on related workers have adjusted to extra precautions and continued on for certain workers unless they were only in administrative roles. We predict that a large volume of companies will embrace hybrid models.

137M[**]

square feet of office space is being sublet, 40% more than last year and the most since 2003.

53[***]

major companies are permanently switching to some form of hybrid work model as of March 20th 2021.

72%[*]

prefer a hybrid remote-office model.

12%

prefer to always work in an office setting,

13%

would like to always work from home if given the choice.

SO, HOW DO YOU SECURE YOURSELF AND YOUR COMPANY WHEREVER YOU WORK?

REMOTE

- Only use approved file transfer, chat, and meetings tools for company business.
- Protect your personal and professional data by knowing what is sensitive and handling it properly.
- Use strong passwords and multifactor authentication wherever you can.
- Verify unusual requests before taking actions such as wire transfers, emailing sensitive documents, or making purchases.
- Take time to review remote workplace guidance from your corporate security team, especially if you’re an infrequent teleworker.

HYBRID

- Incorporate remote and fully physical office best practices into your Hybrid workday.
- Avoid pivoting between home and work computers (especially sending confidential documents or content, or using USB/thumb drives for this purpose). Smash and Grab" break-ins are frequent in many cities when expensive corporate laptops are left visible in vehicles.
- Secure your laptop in your trunk or take it with you if you ever leave your vehicle unattended. “Smash and grab” break ins are always highly frequent in many cities when expensive corporate laptops are left visible in vehicles.

FULLY PHYSICAL OFFICE

- Keep your desk clear of clutter that could grant someone access to sensitive information or accounts like password reminders, office memos, or access codes.
- Have a default screen lock and lock your screen when you leave your workspace.
- Use multi-factor authentication wherever possible.
- Be mindful of your surroundings--look for unfamiliar people or suspicious behavior.
- Don't plug in any device with an unknown origin. Cybercriminals use USBs, charging cables, and other little technological 'treats' as bait to get unsuspecting employees to compromise organizational systems.

Wherever you find your office, being secure is just as much about people and process as it is about technical controls. Being cybersavvy begins with a recognition of your particular risks and a readiness to implement appropriate controls. Have questions? Great! That's the first step.

REVEALRISK
SECURE YOUR BUSINESS

[*] A survey by slack of 9,000 workers in six countries
[**] according to CBRE Group Inc.
[***] according to buildremote.co