venn

WHITE PAPER

9 Questions

to Test Your Readiness for a Hybrid or Fully Remote Workforce

Strategies to prepare your organization for a hybrid or remote workforce

TABLE OF CONTENTS

> “Hybrid is here to stay ... and it can be and will be as disruptive as the pandemic was.”
>
> **—EMMA WILLIAMS**
> Corporate Vice President Of Microsoft

INTRODUCTION

The hybrid form of work – aka work some days in the office and some days at home or another remote location – is lauded for all the benefits it provides both companies and employees but is also causing mayhem for many businesses.

Why mayhem? Because business leaders now have an even bigger challenge than before as they must figure out how to best mitigate cybersecurity risks. Hybrid workers are logging in to access client and company data from a wide array of locations on many different devices. This increases the number of vulnerabilities to a company’s technology infrastructure exponentially and catapults data is turning security into one of the top challenges for the leadership of companies of all sizes.

Before delving further into the data security challenges of a hybrid work model, let us first set the scene. The business world is in a state of transition as organizations determine how and where their teams will work most effectively in the coming months and years. There are many decisions that companies need to make, starting with where their workforce will be physically located.

THE THREE PRIMARY WORK MODELS OF THE FUTURE

MANDATED RETURN TO OFFICE

Some companies are taking a hard-and-fast stance about where their employees will work. Some financial institutions are requiring a return to the traditional, five-day-a-week-in-the-office work week. Think Goldman Sachs, Morgan Stanley, JP Morgan. As Morgan Stanley chief executive James Gorman famously said: “If you can go into a restaurant in New York City, you can come into the office.”

As Morgan Stanley chief executive James Gorman famously said: *“If you can go into a restaurant in New York City, you can come into the office.”*

Many employees, however, are fighting this type of arrangement. There is a very real possibility that companies could lose talent – and already are doing so – if they do not allow employees some flexibility in their work location. We’re curious to see how this group of companies retains its workforce and how they adjust based on employee feedback and departures. Companies that utilize this approach will have the most straightforward opportunity to button up security. It’s much easier to ensure to take the needed precautions to prevent cyberattacks when all employees are logging into the same corporate network using company-issued devices. It will be like 2019 all over again.

FULLY REMOTE

Some companies are looking at the exact opposite model, one that is fully remote. Organizations adopt this approach for various reasons, whether it is to slash costs by eliminating real estate expenses, embrace offshore workers or to satisfy employee requests for greater work + life flexibility. While this work style does cause security concerns, the risks are somewhat mitigated as there are new ways to secure fully remote workers on any BYOD laptop.

Hybrid is perhaps the best of both worlds.

HYBRID

Arguably the most complicated arrangement, but one that continues to gain a tremendous amount of momentum, is the hybrid model. Hybrid gets thumbs up from companies and employees alike. Interestingly, it is viewed favorably among entities that range in size from the largest global corporations (Unilever, PricewaterhouseCoopers, Target, Google to name but a few) to the smallest of businesses across all industries.

Hybrid is perhaps the best of both worlds, as companies can cultivate and foster culture via in-person collaboration, yet also enable employees to enjoy 2-3 days a week of non-commuting, focused work time. This arrangement, where employees and corporations must constantly shuffle their workspace between multiple locations, is fraught with the most potential problems.

IS HYBRID REALLY MORE COMPLICATED?

The hybrid model benefits employees and employers alike. In the simplest terms, employees embrace the flexibility that comes with such an arrangement while companies have the potential to reduce their physical footprint and thus lower some fixed costs. Plus, these forward-thinking companies are keeping employees happy. As we are quickly learning in this time of recruiting challenges, the importance of keeping a workforce happy and productive cannot be overstated.

HOWEVER, THERE ARE A NUMBER OF SIGNIFICANT CHALLENGES COMPANIES FACE WHEN IT COMES TO MAKING THE HYBRID MODEL SUCCESSFUL:

1. THERE'S NO EASY-TO-FOLLOW INSTRUCTION MANUAL

We can all agree that no two companies are structured the same way. Therefore, there is no singular model that will work for every company that aims to take its workforce hybrid. A company must craft a customized solution that works for its culture, leadership team, employees, customers, and extended stakeholders. For most organizations, this won't be easy.

2. CORPORATE LEADERSHIP MUST TAKE A PROACTIVE ROLE

If leaders don't step up and make the success of the hybrid model a priority, it won't be. Extensive planning is needed, robust security systems must be established, and training must occur. Again, this takes work and resources, and certainly isn't a walk in the park.

3. CORPORATE SECURITY BECOMES MORE COMPLICATED

As we think about workers regularly transitioning between secure office environments and their vulnerable remote work locations, taking their devices and digital files with them back and forth, the increased risk of a cyber disaster becomes evident. The probability of a negative outcome is great if the needed protections are not put in place.

FIVE WAYS TO ENSURE DATA IS SAFE AND SECURE IN HYBRID OR REMOTE-FIRST

Corporations need to do their best to ensure all devices and equipment – especially those used at home or in a remote office location – are secure.

1 Implement robust cybersecurity measures.

Be proactive about your company's digital security – don't wait to take action only after a problem occurs. Have an expert, whether internal or external, review how employees work, where they work, and what devices they use to raise the awareness of potential vulnerabilities before they escalate into serious issues.

2 Continuously monitor, measure, and upgrade cybersecurity protections.

Putting a plan in place is an excellent first step, but hackers are constantly upping their game. A steady stream of potential new vulnerabilities will always crop up as cybercriminals become more sophisticated. A system must be in place to address these unforeseen threats.

3 Educate your workforce about the importance of cybersecurity.

Document security guidelines and ensure protocols are properly in place. Emphasize to employees why cybersecurity must move to the top of the list of businesscritical issues to address. And ensure the team knows it can just take one weak link – just one person within the organization who opens a phishing email or similar bait – to bring the company to its knees.

4 Remain vigilant about keeping cybersecurity at the forefront of your company.

During the pandemic, there was a time when all that mattered to companies and employees was getting work done – how, where and on what device didn't matter. It's a bit frightening for many companies to admit this, but it's true – for a time in 2020, security was put on the backburner. But the days of pandemic-related security complacency are quickly ending

5 Understand corporate technology and security teams are running tired and are working overtime.

Security professionals have had so much to deal with since the start of the pandemic. They have been responsible for ensuring that all employees could work seamlessly from home at the drop of a hat. Finding new talent trained in this field is difficult so there's not a huge inflow of help in this area.

WHERE DO YOU GO FROM HERE?

Make it a priority to rethink your cybersecurity policies and priorities, especially if you are moving toward a hybrid work model.

WE STRONGLY SUGGEST A NEXT STEP YOU CAN AND SHOULD TAKE:

Develop a strategy, and then invest in needed resources to ensure your employees keep client and company data secure. And don't hesitate to turn to outside experts to help. It's especially important to dedicate the needed planning and funding to these efforts since there is no "one-size-fits-all" approach to set up and maintain a secure environment for all your employees, no matter their location or chosen device.

The first, and often most important step is simply acknowledging that you must take action.

Following right behind is the need to determine what actions you must take to shore up cybersecurity in your organization.

Do everything you can to build a strong foundation, so your chosen work structure is successful for years to come.

THE HYBRID WORK RISK ASSESSMENT

Many well-known and well-respected business leaders tout the benefits of hybrid and remote-first models. But it's the actual number of companies moving in this direction that has caught our attention. We see the data as proof there is tremendous traction to move to embrace remote work and we see it as the prominent work model for the future.

While the numbers are still fluid as far as the actual percentage of companies that will adopt some variation of a "hybrid" model, the data we've seen predicts that the percentage of companies that will adopt hybrid for the long-term falls in the 70-85% range.

Take our short 9-question quiz to determine if you are ready to embrace the hybrid model and ensure your company's success in the months and years to come.

TAKE OUR QUIZ

[Each question has a yes/no choice]

01

Has your executive team developed and documented an overall hybrid work plan and strategy?

02

Is there a communications plan in place that explains to your team how the hybrid model will work within your organization and outlines the expectations of all employees?

03

Does your company have clear, documented cybersecurity guidelines that the entire organization faithfully follows?

04

Is your team trained to spot and take appropriate action when they recognize potentially malicious communications?

05

Does your team understand how and when to report security issues to the appropriate person or department in your organization?

06

Are password policies simple and efficient for employees to use, and do they include security measures such as multi-factor authentication?

07

Can employees seamlessly and securely move back and forth between an on-site work location and a remote location?

08

Do your organization conduct security audits on a regular basis to ensure your company stays ahead of all regulatory requirements?

09

Does every member of your organization have full confidence that all data is safe and secure – no matter where employees work, and regardless of the type of device they use?

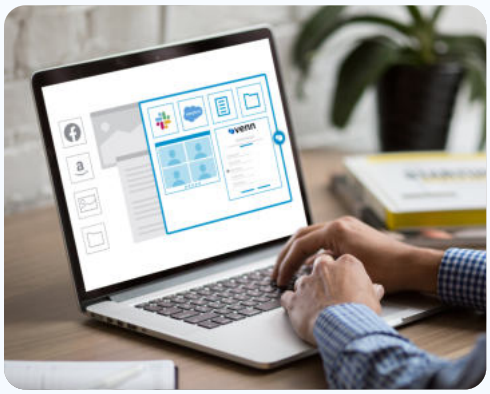
If you answered **“no”** to even one question, we highly recommend you take immediate action to shore up your hybrid work arrangements. **The longer you wait, the higher your risk for a security breach.**

INTRODUCING VENN: A NEW SECURE WORKSPACE FOR REMOTE WORK

VENN IS THE FIRST PURPOSE-BUILT PATENTED TECHNOLOGY FOR SECURE BYO-PC.

Venn secures remote work on any unmanaged or BYOD computer with a radically simplified and less costly solution than virtual desktops or having to lock down every PC. Similar to an MDM solution but for laptops – work lives in a company-controlled secure enclave installed on the user's PC or Mac, where all data is encrypted and access is managed.

Work applications run locally within the enclave – visually indicated by the Blue Border™ – where business activity is isolated and protected from any personal use on the same computer.



Company data is now protected without having to control the entire device, and as a result, remote work is secured without the cost, complexity and performance issues of VDI.

As happened in the past with mobile phones, employees want to use their preferred computer – not have one for work and one for personal – while companies are eager for ways to avoid buying, shipping and locking down computers. With Venn, Secure BYO-PC technology is now a reality.

Over 700 security and compliance-driven organizations, including Fidelity, Guardian, and Voya, trust Venn to meet FINRA, SEC, NAIC, and SOC 2 standards.

NAIC FINRA AICPA SOC HIPAA COMPLIANT

venn

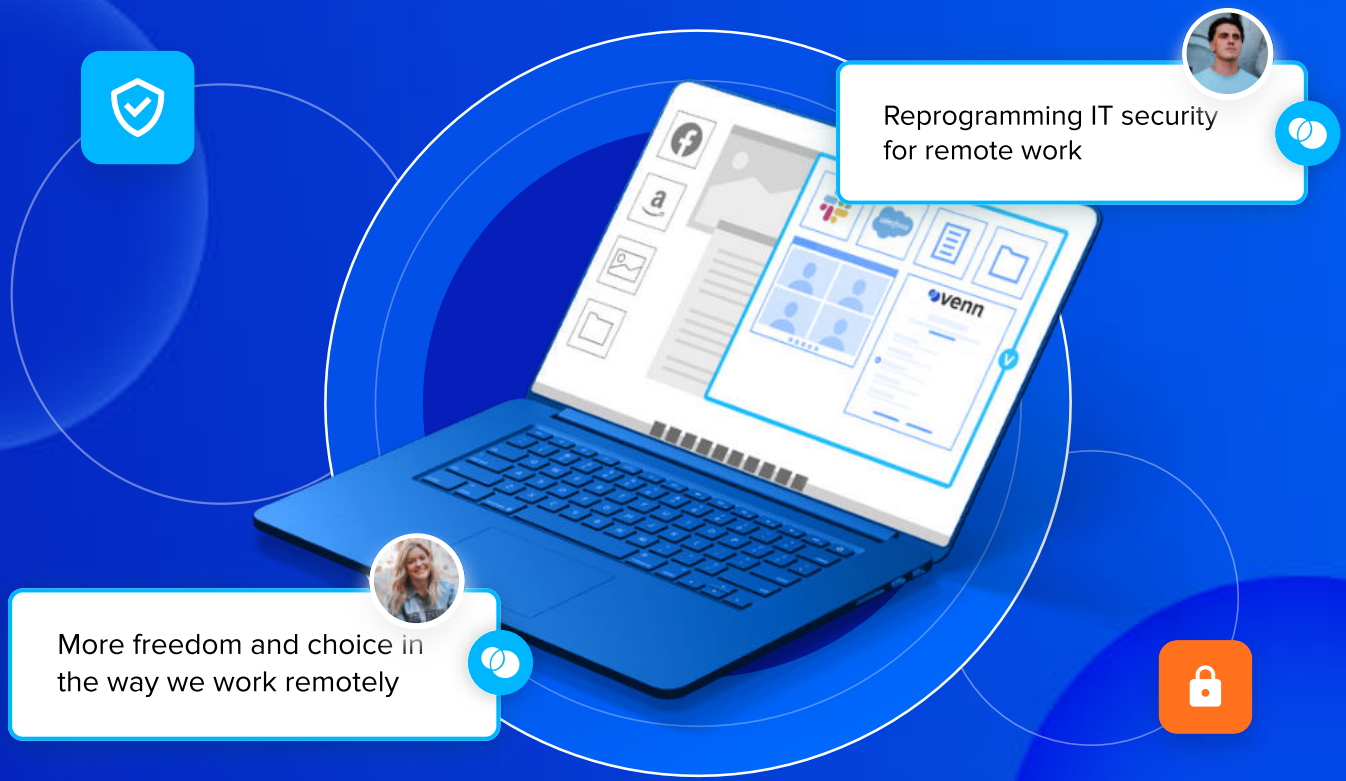
Take the next needed step.

Discover Venn.

> By using Venn, we can leverage our time and talent to help our advisors be more successful. The solution helps Spire and our advisors compete with the larger firms by leveraging the same technology and levels of data security.

David Blisk
CEO Spire Investment Partners

Book a Short Demo >



Website Blog Linkedin