FREE REPORT:

The Small Business Guide to Working From Home

Learn the Key Items You MUST Do to Safely and Securely Allow You and Your Employees to Work Remotely

By James Pearson

President, The Computer Center

www.computer-center.com

Phone:608-755-1524

A Letter from The Author:

Why I Created This Report And Who Should Read It

From the Desk of James Pearson
President, The Computer Center

Dear Colleague,

At the outbreak Corvid-19 our office began fielding a flood of calls about how to quickly implement a work from home strategy to meet the government demands and CDC recommendations. Customers who had never considered any kind of telecommuting or remote work strategy were suddenly being forced to find alternative ways to keep the doors open and keep employees productive without actually being in the office.

That's why I wrote this report. **I wanted to give CEOs a simple, straightforward guide that not only answers your questions in plain English, but also provides vital experience-based information that most IT companies don't know (or may not tell you) that could save you and your company hundreds, if not thousands of dollars in lost productivity, sales, and even expose your company to Data breaches and security risk if not implemented correctly**

My name is James Pearson, author of "**Essential Cyber Security for Your Small Business: How to Protect Your Small Business from Cyber Attacks, Hackers, and Identity Thieves Without Breaking the Bank**", and President of The Computer Center. My organization has been providing IT services in Janesville and the surrounding area since 1983. While you may have never heard of us, I hope that by the time you finish this report, you'll be glad you finally did.

The simple fact is that before you implement a work from home strategy you must fully understand the pros and cons to avoid making some VERY poor and expensive decisions that you'll deeply regret later. The information in this report will arm you with the critical facts you need to avoid expensive, time-consuming mistakes.

Of course, we are always available as a resource for a second opinion or quick question, so please feel free to contact my office directly if I can clarify any points made in this report or answer any questions you have.

Dedicated to serving you,

The 10 Things You Must Consider BEFORE You Implement Your Remote Work Plan

Who will be working remotely?

Different employees need different tools and access to different resources. It may not be necessary, or even realistic to have all your employees working from home. In our current situation, with Covid-19, symptomatic people are asked to self-quarantine. You may also want to ask people that have recently traveled to stay home as a precaution.

Of course, not everyone in your company may be a computer user, especially in manufacturing businesses or retail situations.

What resources will they need access to?

Every business is unique and the resources you need to access while out of the office will greatly affect how your IT company sets you and your staff up. For example, if you have an in-house server with a software program that runs your company such as a specialized accounting or quoting tool, your IT company may need to configure remote access to each person's computer.

Meanwhile, if you predominately work with software that is already Cloud-based, or simply need access to Word and Excel documents, working from home may not require remote access at all.

How will you control access to sensitive data?

When you sit down with your IT company to make a plan to work remotely, even in the face of an immediate need like the Corona Virus pandemic, you need to think about the long-term affects of allowing people outside your physical building, possibly using their own computers and own Internet, access to your company data. This data may contain items covered by privacy laws, or simply business trade secrets such as client lists, procedures, and proprietary information that you would not want released to anyone outside your organization.

What will you do to control data breaches?

So, how do you protect your data from breaches while keeping your employees productive remotely? A data breach is the intentional or unintentional release of data. Even if you have faith and trust in your employees, you still should consider how you can best protect your data from breaches, even accidental ones.

How will you protect your employees and corporate data from viruses and malware?

Unless you are providing every employee with a company-owned laptop or phone, over which you and your IT company have strict control, chances are that your remote employees will be using their own home computers to access your data.

This exposes your files and network to a new kind of risk. Since most home users are significantly laxer about security than most companies, you'll need to determine how to protect your data if it's being accessed by computers out of your control. Will you require they provide certain levels of protection, such as enhanced antivirus software? Will you cover that protection?

How will you collaborate?

If your team is accustomed to working as a group, then isolating everyone can pose some challenges. How do you have staff meetings? What do you do without your whiteboard? Instead of dialing someone's extension or walking down the hall, how do you get feedback or hand off tasks to your staff?

How to plan for the worst?

Today's current situation is uncertain at best. Some reports say that these conditions might last for months! What this means is that whatever approach you take to working remotely, you have to consider the long-term costs and possibilities. These means discussing your long-term plans to continue doing business remotely. How will you present your solution to clients? How will you're team communicate? What will your schedule look like?

Are there any mandated security or privacy protections you must consider, such as HIPPA?

The remote work solution that you put in place will need to meet any requirements and regulations for your industry. Allowing employees to use personal computer equipment, phone lines, and Internet connections while working from home may not be allowed. Be sure to discuss these with your IT provider before you implement your strategy.

What about the Internet?

The quality of your business internet connection and your employees' home Internet connections becomes significantly more important when you and your team begin working from home. It will also affect how your IT provider gets everyone connected and accessing your company resources. Some remote connection software handles slower connections better than others.

What about 2 Factor Authentication?

Two Factor Authentication (2FA) is one of many security features you need to consider as you migrate to a remote team. 2FA adds an additional layer of security by requiring you to enter a secondary piece of information, such as a code sent to an email address or texted to your phone, to verify your identity.

Remote Work Pre-Planning Checklist

Complete this checklist and share it with your IT professional to help implement a remote working solution that best fits your needs.

_____ Are you bound by any specific privacy or security regulations such as HIPPA, SCR 20, GDPR, etc.?

_____ Do you need access to files such as Word, Excel, Powerpoint?

_____ Do you have an application that runs on a server or host computer and <u>not</u> in the Cloud? Examples would be QuickBooks or an industry specific piece of software for quoting.

_____ Is your office Internet connection fast enough? Your Internet must be able to handle both high download and upload speeds. Connections such as those by the cable companies are geared towards fast downloads, but don't always provide as much bandwidth for uploading data, which is needed to send data to your remote workers.

_____ Do you have a static IP address? Your IT company can assist in answering this, but you may find it on your Internet provider's bill. A static IP address for your company makes it easier to get your staff connected back to the office.

_____ How will you handle phones? Is your solution a VoIP system that can easily be taken home with each employee, or will you need to arrange to have phone number forwarded?

_____ How will you collaborate and have meetings? Will you use a conference calling service or a product like Microsoft Teams?

_____ Do you need to print remotely?

_____ Is your employees' home Internet fast enough?

_____ Will you need to provide employees with laptops or other equipment?

_____ What are your security concerns? Will you need to provide monitoring of employee devices? Extra security and protection?

8 CRITICAL Characteristics You Should Absolutely DEMAND From Any IT Professional You're Considering To Set-up Your Remote Office Technology; DO NOT Trust Your Infrastructure To Anyone Who Does Not Meet These Criteria!

There is no "one size fits all" solution; the best solution is depends on your specific business needs, the applications you use, how many people will be accessing your systems remotely, the available equipment and dozens of other factors. **That's why you want to look for a consultant who meets the following criteria:**

1. **Look for a consultant who has experience setting up remote access and STRONG (and recent) client references.**

<u>Do you really want to be the person who "pays" for your consultant's training?</u> I've found that the price to correct problems created by novices is much greater than the cost to do it right the first time with an experienced technician. Ask for *recent* references and call them! Past performance is generally a good gauge of future performance.

2. **Make sure they do a THOROUGH evaluation up front**

If your consultant doesn't insist on doing a thorough evaluation BEFORE handing you a proposal, do NOT hire them! If they don't do their homework they could easily sell you the <u>wrong solution</u>, causing you to have to spend <u>MORE money, MORE time, and have MORE frustration getting to what you really need</u>. Most consultants will do a quick, cursory review and provide a free recommendation (proposal) because they want to close the deal fast. Here is a short list of the things they should investigate or ask you:

- What are your overall goals and specific objectives for allowing your employees to work from home or on the road?

- How many employees will be working remotely? Will they be accessing the network at the same time or at different times?

- What applications (including specialty or proprietary apps) and data will your employees need to access?

- What type of devices will your staff use to access the network? (Home computers, PDAs, Blackberries, laptops, etc.)

- What type of Internet connection will be available on the sending AND receiving end?

- What levels of security do you want in place?

- What level of monitoring do you want in place? For example, are there certain web sites and content you want "off limits?"

- Will the remote worker need to print documents?

- What are your long-term plans to keep your business running?

3. **Make sure they can TRAIN you and your staff.**

So many computer consultants are great at installing the "stuff" but <u>fall short on training you and your staff how to use the great "whiz-bang" technology they've just sold you</u>. Make sure you hire someone who is able and willing to do the "hand holding" required when installing any new process or technology…we're only human after all.

4. **Make sure they can provide help desk suport.**

One of the main appeals to teleworking is the ability to work at night or on weekends; that means <u>you need someone to be "on-call" during those off-peak hours if you or your employees have technical problems logging in or accessing the network</u>. Bottom line, if you're your consultant doesn't offer after-hours support, don't hire them to do the job. There is no benefit to having remote access if you have to wait until Monday or 9am the next day for support. Look for a company with a dedicated help desk.

5. **Make sure they INSIST on maintaining the network**

<u>Virtual office networks require more 'care and feeding' to make sure they work properly and stay secure</u>. You cannot "set it and forget it" or you're asking for problems. Only hire someone who is prepared to perform regular check-ups and updates of your network, usually under a maintenance or managed services plan.

6. **Look for someone who can also solve the phone piece of the puzzle, not just the network access piece.**

If you want your work-from-home employee to be able to make and receive calls <u>and APPEAR as though they are in the office to the caller</u>, then look for someone who can set up your phone system to work with your remote employee's home phone or cell phone. Usually this can be accomplished with VoIP technology (Voice Over Internet Protocol). Confirm that whoever you hire can either provide these services or has a partnership with a reputable vendor who has this expertise.

7. **Make sure your consultant is willing and able to be a vendor liaison for your specific business applications or other specialty applications.**

It's amazing how many critical applications work fine within the office network, but then slow down or shutdown when accessed through a remote location. It's important to <u>ensure your consultant is able and willing to confirm your applications will operate efficiently remotely, which means they may need to get on the phone with the help desk of one or more of your software vendors</u>.

8.   **Look for a consultant that has expertise in setting up employee monitoring and content filtering.**

It's more difficult (but not impossible) to protect company secrets and proprietary information when it's stored on a location outside of your office. Therefore, make sure the company you hire has expertise in setting up and managing content filtering and security for remote machines.

<div style="border:1px solid #000; padding:1em;">

Not Sure If You Are Ready to Set Up Remote Access?
Our Free Remote Access Consultation Will Help You Decide

As a prospective client, we'd like to offer you a free Remote Access Consultation. At no charge, we will have a brief call to review your situation, discuss your business practices and needs and provide recommendations on how you can quickly and easily set up remote access for you and your staff.

We will also discuss your options, clarify any grey areas, and answer any questions you have. We will also map out the costs and steps involved so you know exactly what to expect.

You are under no obligations to do or buy anything; this is simply our way of introducing our services to you and demonstrating how we can make your remote access project a complete success.

To schedule your free consultation, call our office today at 608-755-1524* or send an email to sales@computer-center.com

</div>

*Offer valid for businesses in the Southern Wisconsin/Northern Illinois market only, and may be limited.