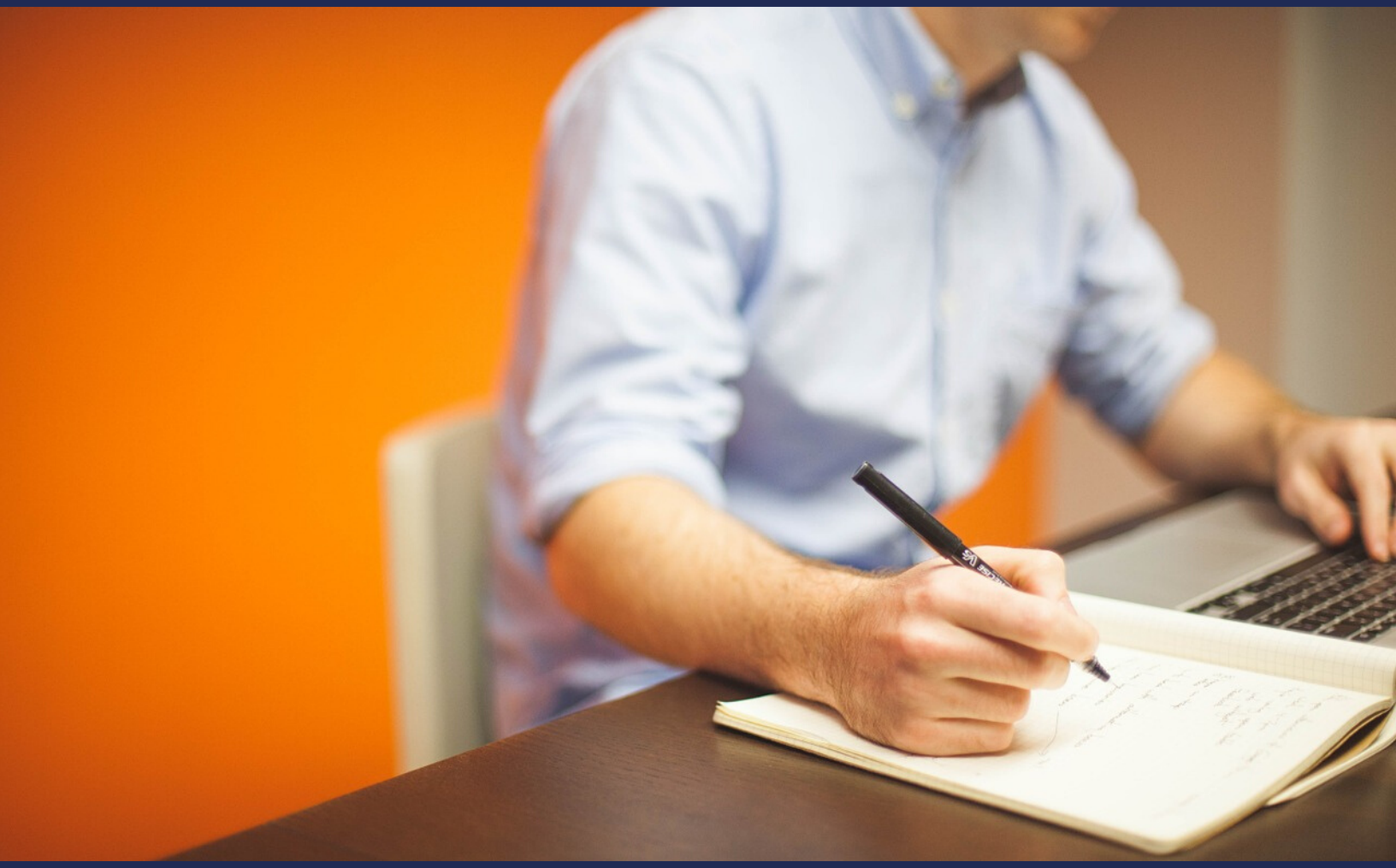
thinkCSC's Guide to Remote Workforce Security



think CSC | Your Chief Technology Office

REMOTE WORK IS HERE TO STAY

The 2020 pandemic may have precipitated an unprecedented number of employees working from home, but as we consider how to maintain the safety and health of our employees and customers going forward, supporting a remote workforce will continue to be one of the most important methods in which we can do so. While more companies are opting to have their employees work from home as a necessary way to achieve business continuity, it will almost certainly be a practice that continues long after the stay home orders cease. Taking action now to develop a long-term remote work strategy will benefit your organization whether you continue to have most of your staff work from home or simply want to have it as an option for attracting top talent in the future.

80% of employees want to work from home at least part of the time

Global Workplace Analytics

REMOTE WORK DEMANDS TOUGH SECURITY

As you develop your remote workforce plan, you should consider areas of workforce management, such as:

- flexible scheduling
- productivity
- meeting and event management
- maintaining employee engagement and satisfaction

Technology and IT infrastructure will be critical elements. In fact, one of the biggest concerns business leaders and IT support teams will need to address when supporting a remote workforce is **data security**. From ensuring that your secure data doesn't land in the wrong hands, to maintaining relevant data with the appropriate employees, identifying which employees need access to what information is a crucial first step.

To effectively support remote workers, you'll need to consider their physical environment - the space in which they have to work - as well as their technical capabilities (internet access, infrastructure, security).

EMPLOYEES WITHOUT SUFFICIENT SECURITY ARE EASY TARGETS

During any kind of crisis, you'll find people stepping up, helping out, and innovating for the common good. But you will also find an increase in the number of people who will take advantage of the most vulnerable. Whether it's a pandemic or just tax time, criminals will take advantage of perceived vulnerabilities.

CRISIS EMBOLDENS CRIMINALS

During the COVID-19 pandemic, there was a significant increase in phishing attempts. Hackers sent emails promising cures and treatments, created fake websites designed to trick people into providing personal information, and even hacked into hospitals to try to get ransom money by holding patient data hostage. According to Google, there was a **350%** increase in phishing websites during the pandemic. Many of the sites were COVID-19 websites promising quick cures or treatments in exchange for personal information.

TELEWORKING SAFELY

Even before the pandemic, employees who worked from home were not always employing best practices for keeping data secure. Whether they are using public Wi-Fi in a coffee shop to access your network or do not have sufficient security on their home Wi-Fi to reasonably protect themselves from cyber attacks, hackers are eager exploit your remote staff. They are trying to find any weakness that will give them access to your data - and without the protection of an enterprise-grade network, your employee is an easy target.

It's more important than ever to make sure your employees have access to information about these risks. We urge you to communicate with your teleworking employees to make sure they are aware of these risks and are taking the appropriate security measures to protect your data and network. Establish routine methods for alerting them to the latest risks and guidance.

PERSONAL INFORMATION THEFT COMPROMISES BUSINESSES

Why do hackers work so hard to obtain personal information? They know that most people reuse passwords in multiple places, so that once they have an employee's personal information, they have likely also gained access to your corporate data. An employee may have used the same password for their grocery app that they use to access a business app. Requiring the use of a password manager and multi-factor authentication is essential to protect your organization from this risk.

GUIDE TO ONLINE SAFETY FOR REMOTE WORKERS

When remote workers use their home PC for teleworking purposes, a whole new set of challenges arise when it comes to security. Make sure you're following these best practices:

- Every employee should be required to have security software installed and fully activated on their PCs. Provide it for them if necessary.
- Businesses should limit network access to only that which employees must have access to in order to perform their duties.
- Ensure that a current antivirus platform is installed on every device they might use.
- Make sure the operating system on their device is up to date and fully patched.
- When not in use by the person working from home, ensure that the user's session is logged off, preventing anyone else in the home from accessing business applications.

While phishing and similar attacks will be on the rise, overall systems security will also be tested with the increased remote workforce.

REMOTE WORKFORCE SUPPORT

Supporting your remote workforce goes beyond technology, but you simply cannot ignore the IT security and infrastructure needs of your team if you want to stay in business, protect your data, and avoid unnecessary risk.

TOOLS TO PROTECT YOUR DATA

VPN - The purpose of a VPN is to provide you with a secure network from which you can access your office applications over the public internet. A VPN creates a private connection, or tunnel, through the open internet. The idea is that everything you send is encapsulated in this private communications channel and encrypted so that even if your packets are intercepted, they can't be deciphered. You may need to add more licenses to full support the number of people using your VPN - but they should all be accessing your network via the VPN.

MFA - MFA is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authenticating mechanism. Two-factor authentication, or 2FA, is a method of confirming users' claimed identities by using a combination of two different factors: 1) Something they know, 2) something they have, or 3) something they are.

REMOTE WORKFORCE TECH REQUIREMENTS

It's important to realize that while some organizations have had remote workforce policies in place for some time, many organizations will be learning to manage a remote workforce for the first time. And on top of that, this need for a remote workforce was driven by a global pandemic that didn't just upset work but every aspect of your employees' lives. They may have lost loved ones unexpectedly; they may be suddenly thrust into supporting children who are distance learning; they may be sharing the space with a partner or spouse who has also transitioned to remote work. They may be recovering from being ill themselves.

END USER TECHNOLOGY

Does your staff have the appropriate equipment to work from home? Devices? Adequate internet access? You may need to configure their device or provide one for them, especially if their device is incapable of supporting the apps you need them to use. Do you have endpoint security that will prevent them from connecting? What about workers whose jobs can't be done remotely?

CORPORATE NETWORK SECURITY

Do you have a procedure in place to handle users who fail your security requirements? Even if you are able to increase the number of VPN licenses, do you have the necessary bandwidth to handle all of the remote connections? Do you have the IT support in place to answer questions and resolve issues for your remote work teams? Where will help desk staff be located?

Is Zoom Secure?

thinkCSC suggests switching to a more mature product with greater security built in. If that's not possible, here are some tips to help make meetings more secure.

- Make sure to always update your Zoom product when asked.
- Don't publicly share your Zoom "Meeting ID." Send it directly to the people you want on the call.Set a password for the meeting, then share that only with the right people.
- Make sure "screen sharing" is set to "Host Only." That prevents other people on the call from abruptly blasting text or images onto the other participants' screen — a favored tactic of "Zoombombing" trolls.
- Use the "waiting room" feature. It prevents new participants from joining the call until the host approves.

THINKCSC REMOTE WORKFORCE SOLUTIONS

Cloud Hosting

Our cloud services provide the access your employees need while keeping your data secure. From hosted email that you can access from anywhere on any device to mobile device management that ensures data security, thinkCSC cloud services provide your organization with the necessary protection that lets you offer flexible work programs while still providing you with peace of mind.

VoIP

Don't miss calls from your customers. VoIP is more than just a phone system. thinkCSC's hosted VoIP is a complete customer service system as well, allowing you to:Assign dial-in codes that put clients in touch with your on-call team.Set up calls so that voicemail is delivered anywhere that is convenient, from your cell phone to your laptop. Maintain consistency across multiple locations, by having a single number with assigned extensions that reach your team members wherever they choose to have their calls delivered.Manage calls and voicemails without sacrificing security.

Office 365: Anywhere You Want It

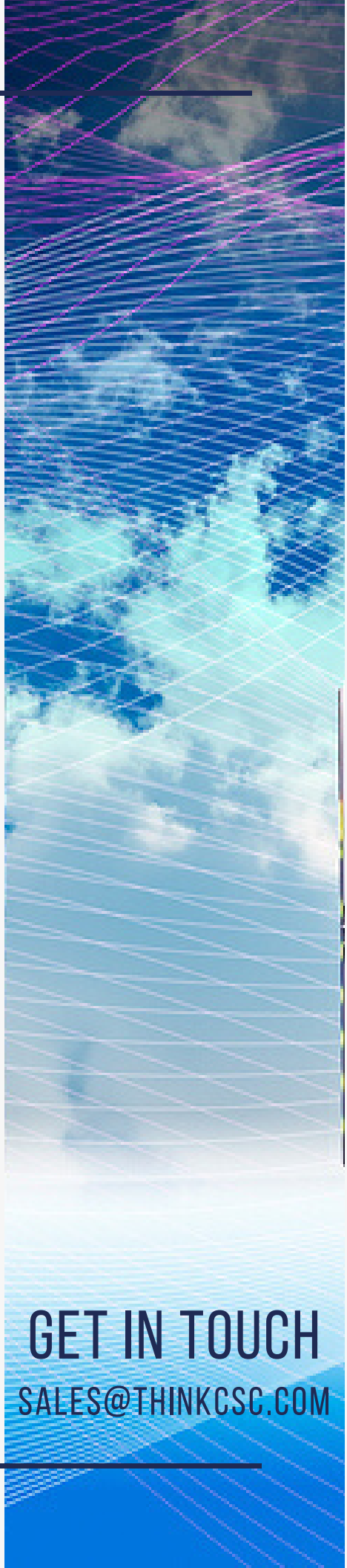
Your team can work remotely virtually anywhere. We'll ensure that they can access documents when and where they need them and get the same experience using any mobile device. Office 365 is a powerful tool for business continuity in the age of a pandemic.

We can assist remotely with your PC, Mac, or mobile devices, troubleshoot network or server issues, install and upgrade software, or take care of simple tasks, such as resetting passwords or authorizing data access. And, because problems can arise at any time, our support personnel are just a phone call away for your convenience.

PARTNERING WITH THINKCSC

thinkCSC has more than 20 years of experience helping clients exceed their goals. We understand that business and technology are so intertwined that you can't be strategic about one without the other. We offer customized and bundled outsourced IT services you need to achieve your objectives; increase efficiency, productivity, and agility; cut down on IT costs; and ensure you have a competitive edge. Whether you want to outsource most or all of your infrastructure management, or if you simply want to optimize the systems already in place, thinkCSC provides personalized IT expertise that saves money and provides the manpower that ensures your infrastructure is always an asset – never a liability.

At thinkCSC, we believe that in order to achieve maximum success, regardless of the size or type of your organization, you must make IT an integral part of your overall business strategy and partner with IT professionals who not only understand how to leverage technology to their advantage but who are also committed to understanding your business goals and aligning your IT strategy to theirs. We pride ourselves on having the best business-savvy technical experts in the industry. If you would like to learn how to create an IT security strategy aligned with your organizational goals, contact thinkCSC for more information.



GET IN TOUCH

SALES@THINKCSC.COM